A Human-Centred Approach to National Identity Management Systems

I, Pengiran Adrian Pengiran Salleh AB Rahaman, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Pengiran Adrian Pengiran Salleh AB Rahaman
University College London
Submitted for a PhD in Computer Science

ABSTRACT

This thesis explores the concept of a human-centred Identity Management System (IDMS), and how it can be implemented by organisations. The review of the literature on previous approaches to identity (i.e. privacy, trust, and usability) reveals that claims of IDMS being 'human-centred' are rhetorical; in reality, organisations' administrative convenience is prioritised over the needs of individuals who are treated as purely functional components within the IDMS ecosystem.

The research conducted to build a human-centred identity concept involved three separate studies, each approaching the question of identity from a different perspective. Study 1, the system study, focused on the design of IDMS and its impact on individuals' everyday lives. A total of 14 different past and present N-IDMS implementations were analysed using thematic coding. The result of the study was the development of a framework that expressed a system in terms of a set of *structural and metrical design properties*, and how these can shape the individuals' *lived experience* of identity.

Study 2, the individual study, explored individuals' perceptions and initial acceptance of N-IDMS. Grounded Theory analysis was applied to the data from 15 focus group discussions (groups consisted of 3 participants who were all either of British, Indian, or Bruneian nationality). The study revealed that individuals' decision to accept an IDMS are influenced by their *situation perception*, *system judgment*, and *concerns*. These findings were further refined through the use of a survey study. The individual study also explored the impacts of National Culture on individuals' perception of an IDMS.

Finally, the third study took an organisation-centric approach, through the analysis of documentation and interviews on the current N-IDMS implementations in 3 different countries (UK, Brunei, and India). Exploring identity as a strategic resource, the study developed a set of organisational requirements around the *identity creation* and *identity application* processes, which have an influence the design of the IDMS.

The main contribution of this thesis is the development of a unified framework that provides a complete narrative of the identity situation, from planning and design to individual perceptions, as well as the impacts on the *lived experience*. The findings of this research have been validated through the use of *expert evaluations,* which have found the framework to be complete and useful for both practitioners and researchers.

Acknowledgements

I am indebted to my supervisors and examiners over the course of this PhD. None more so than my primary supervisor, Professor Angela Sasse, who has been a great source of guidance and support throughout the process. Thank you for going above the call of duty, especially in the final few months leading up to the submission.

Acknowledgement also goes out the government of Brunei Darussalam for sponsoring my research, and providing the opportunity to explore and contribute to the field, and hopefully to the future development of the country as well.

To my colleagues, I thank you for putting up with some of my quirks in the research office. Rest assured that as I move on, you should now have the peace and quiet necessary to pursue your own work.

It also goes without saying that I am deeply thankful to my family who has continuously spurred me on. My parents, who have been a great source of encouragement, pushing me forward, especially when I have doubt in myself. My brother and sister who have always been able to bring a smile to my face.

Finally, I would just like to acknowledge the unexpected joys of life itself. Had it not been for my PhD, I would not have met the most amazing woman. But I did, and I fell in love with her. She has become my new light, my new centre. Thank you, Noorsurinah Tengah, for coming into my life.

Table of Contents

Table of Figures

Glossary - The Identity Ecosystem

The following is a brief overview of the terms used throughout this thesis. While Identity Management Systems can be quite diverse, the structure and definitions of here are based on the cases reviewed in this thesis.

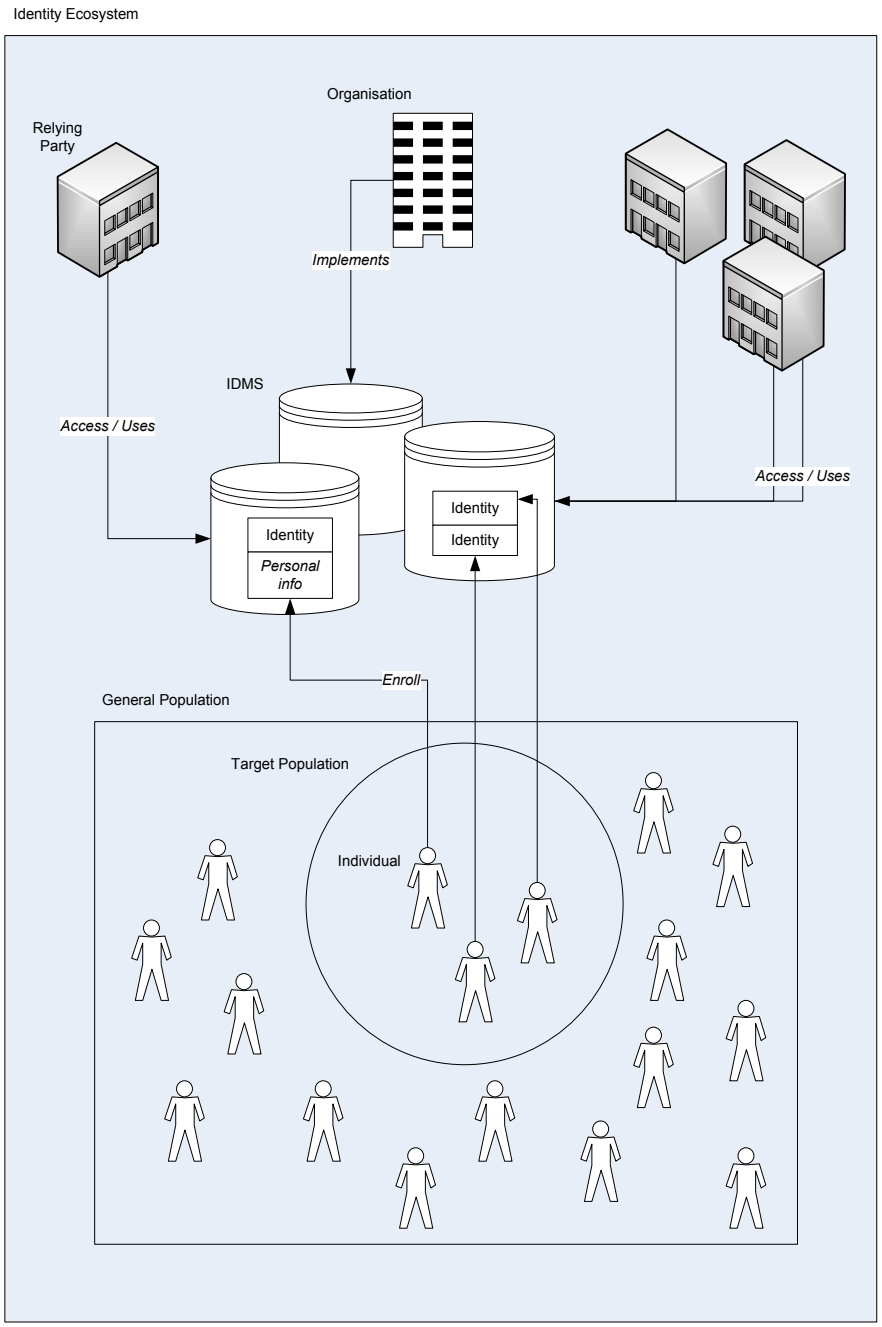


Figure 1 Identity Ecosystem

Table 1 Glossary of terms used in this thesis

Term	Definition
Identity	A set of information and attributes about an individual that is collected and stored, linked to an identifier(s) that sufficiently identifies the individual within a set of individuals.
Identity Management System (IDMS)	A mechanism that allows for the creation, administration, access, and use of identity.
General Population	All the people that act within the context of the IDMS; this includes people who operate in the context, but may not be enrolled within the IDMS.
Target Population	The section of the general population is required to enrol with the IDMS so as to continue to operate within the context.
Individual	A single person from the target population that has enrolled with the IDMS.
Organisation	The entity that is in charge of planning, developing, running, and maintaining a particular IDMS.
Relying Party	An entity that requires access to the IDMS.
Human Centred IDMS	An organisations implementation of an IDMS that views individuals as major stakeholders, and therefore addresses their concerns and negative perceptions, while also accounting for the lived experience.

Chapter 1: Introduction

> *"The explosive entry of technology into every aspect of life has changed how people live, how they work, how companies do business – and how governments serve their people."* (Silcock, 2001)

Identity is a construct that underlies the mechanisms, which enable or prevent individuals' from performing any action in a social environment. As such, many organisations seek to obtain - explicitly or implicitly - reliable proof of individuals' identities, enabling them to ensure effective policing of their rules and policies. Ashbourn (2000) describes how administrators in ancient Egypt used anthropometric techniques to identify workers claiming their food rations to prevent them from collecting rations more than once. Anthropometric techniques were also used in France as a means of identifying recidivists, so authorities could give them harsher sentences than first time offenders (Caplan & Torpey, 2001). Today, individuals' possess various forms of identity documents, such as passports and driving licenses that are accepted as official proofs of identity.

But with the increasing spread of IT systems, there is a growing *disembodiment* of identity processes; interactions between individuals and organisations that were previously conducted face-to-face, and that admitted the use physical documents as evidence, are now mediated through information and communication technology (Giddens, 1991; Lyon, 2005). Identity has entered the digital arena, enabling organisations to *re-embed* individuals into relationships that no longer involve face-to-face transactions.

1.1 E-Commerce and Identity

> *"If I have 3 million customers on the Web, I should have 3 million stores on the Web."* (Jeff Bezos, CEO of Amazon.com, in Schafer, Konstan, & Riedl, 2001)

The embrace of the digital representation of identity has empowered organisations to utilise and manage identity in new ways; *"an electronic-based society has dramatically reduced the cost of collecting, storing and processing individuals' personal information. As a result, it is becoming more common for businesses to profile individuals in order to present more personalised offers as part of their business strategy"* (Camenisch et al., 2005). For example, *recommender systems* allow businesses to offer customers personalised product or service recommendations based on the customers' personal identity profile (Resnick & Varian, 1997; Schafer et al., 2001). In the same vein, identity has been utilised to generate trust on the Internet. *A reputation system* is an identity platform that enables customers to rate entities they might come into contact with, which can *"assist other parties in deciding whether or not to transact with that party"* (Jøsang, Ismail, & Boyd, 2007).

1.2 E-Government and Identity

Digital identity is not only utilised within commercial enterprises, but is also being adopted by governments in pursuit of goals in the digital arena. E-Government is seen by many as a mechanism to revolutionise the way governments function; current efforts to make use of technology aim to shed the traditional one-to-many model of government, and migrate to a more efficient and personalised online medium (Layne & Lee, 2001; Silcock, 2001). Identity is the key element that will drive personalisation, as well as enabling the security of online transactions.

> *"A key theme for coming decades in all our case study countries will be identity management, as more advanced online governmental interactions with citizens and businesses rely on the transfer of personal data."* (Dunleavy, 2006)

Governments' desire for efficiency is enabled by the mobility and transferability of digital identities. Citizens interact with the government at various levels and through various agencies, typically requiring the citizen to manage a unique identity with each government body: paying taxes requires an individual to establish a relationship with the tax department, registering a recently bought car requires interaction with the vehicles department, while receiving health care requires the public to establish an identity with the health agency. However, as services are being moved to an online medium, governments are exploring new identity designs that better support their goals (Lips, 2007).

One of the goals of e-Government is to create a *joined-up government* (Tony Blair, 1999), which *"denotes the aspiration to achieve horizontally and vertically coordinated thinking and action"* (Pollitt, 2003). This should enable better information sharing between government agencies, as well as making it *"possible to offer citizens seamless rather than fragmented access to a set of related services"* (Pollitt, 2003). It is often considered inefficient and troublesome to require that citizens have to establish separate identities with each service, and doing so may also lead to *"a problematic patchwork of identity one-offs"* (Cameron, 2005). An integrated or centralised *identity management system* (IDMS) is seen as an essential step in delivering *joined-up government*.

Governments are also interested in the potential administrative cost savings that can be brought about through the use of centralised IDMS. For example, in extending the concept of the UK Transformational Government initiative, better management of citizen information was identified as an important aspect of development. It has been estimated, that improved identity management in the Revenue and Customs department resulted in an estimated £100 million of savings each year (Varney, 2006).

Therefore, in support of their e-Government goals, governments around the world are pushing for the implementation of *national identity management systems* (N-IDMS) (London School of Economics, 2005). An N-IDMS is a nationwide identity scheme, in which all citizens will typically be assigned a unique identity number; this may be further supported by the distribution of identity cards to all citizens, as well as the implementation of a centralised database that holds citizens' personal information (e.g. name, address, date of birth). A citizen can then use this as a proof of identity when interacting with public and private sector organisations. Countries that already possess paper-based N-IDMS are now moving towards a digital platform in their quest for more efficiency, while countries that currently do not have an N-IDMS are attempting to introduce one.

1.3 National Security and Identity

In addition to aiding e-Government development goals, the push for N-IDMS is also fuelled by the climate of insecurity. The terrorist attacks on September 11th 1999 sparked a worldwide security concern; the attacks were followed by huge media coverage that blew the situation out of proportion (Schneier, 2003). But for governments, the feeling of insecurity caused by the extensive media coverage provided a catalyst for the introduction of an N-IDMS. For example, the governments of the United Kingdom, United States and Philippines have all cited the implementation of N-IDMS as a strategy in battling terrorism (Lyon, 2007).

Another of the security benefits of an N-IDMS is that proponents believe that it can reduce illegal immigration (Lyon, 2009). Recent statistics show an estimate of about 30 to 40 million illegal immigration worldwide (Papademetriou, 2005). In the UK alone, the government published a report claiming a figure of 430 000 illegal immigrants, while the size of the illegal population in the US is believed to be as large as seven million (Woodbridge, 2005). Both governments have cited illegal immigration as a factor in introducing an N-IDMS. This is also true for many other governments such as Spain, Malaysia, Hong Kong, etc. (London School of Economics, 2005; Lyon, 2007).

Governments also tend to argue that N-IDMSs will aid in the reduction of fraud. The British government has reported that instances of identity fraud in the UK have risen by over 500% since 1999, to a figure of 135,000 recorded cases (Burnham, 2006). The total estimate of the cost that this has on the UK economy is somewhere in the region of £1.7 billion (Identity Fraud Steering Committee, 2006). Australia's efforts, among others, have typically been driven by its concerns for benefit fraud (London School of Economics, 2005).

1.4 Acceptance of IDMS

While many governments claim that an N-IDMS will make government more efficient, help fight crime, reduce fraud, battle illegal immigration, and combat terrorism (Lyon, 2009), some countries have experienced backlash from citizens when attempting to introduce such schemes. For example, the British and Australian government have recently scrapped plans to introduce nationwide identity schemes, while the plans in the United States for an N-IDMS are facing an uncertain future (BBC, 2010a; Lyon, 2009; Tanner, 2007). Japan and Taiwan have also faced resistance from the public (BBC, 2002; Chuang, 2003).

Not only governments that are facing public opposition, but private entities as well. *Blizzard*, a popular game publisher, recently back pedalled on its controversial plans to use a Real ID system, which forced players to post forum comments under their real names (BBC, 2010b). Within 24 hours of the announcement, the Blizzard forums had received over 1000 highly critical comments; three days later the total number of comments amounted to 50,000, which is when Blizzard announced that it would not follow through with its Real ID plans (Shiels, 2010). Phorm, a personalised online advertisement platform, suffered from some public disapproval, and was the subject of legal proceedings by the European Union (Waters, 2009). Facebook, a popular social networking platform, has also been at the centre of controversy, early on with its news feeds, and recently with its release of personal information to third party developers (Beaumont, 2010).

1.5 Problem Statement

Typical approaches to identity research have focused on the technical security aspects of identity systems, resulting in technically dominant paradigms that do not fully account for the underlying human factors; the identity field is *"almost exclusively tackled from within a technical domain by experts with a dominant background in a technical discipline"* (Lips, Taylor, & Organ, 2005). This technology-centred approach comes at the expense of the human aspects, and therefore do not address the underlying concerns of the identity itself.

A broader view is required in order to identify the human factors that might affect identity systems. For example, what is the lived experience of constantly being asked to constantly prove one's their identity to others (see Chapter 5)? Does the perceived seriousness of a societal problem affect individuals' intentions to adopt an IDMS (see Section 6.3.1)?

This is no trivial task, as identity concerns stem from a complex interaction of various concepts (Figure 2). At the core of this vortex is the multi-facetted nature of identity itself; while most people understand the concept of identity, an agreed definition, from both a layman and research perspective, is difficult to establish (Camp, 2004a).

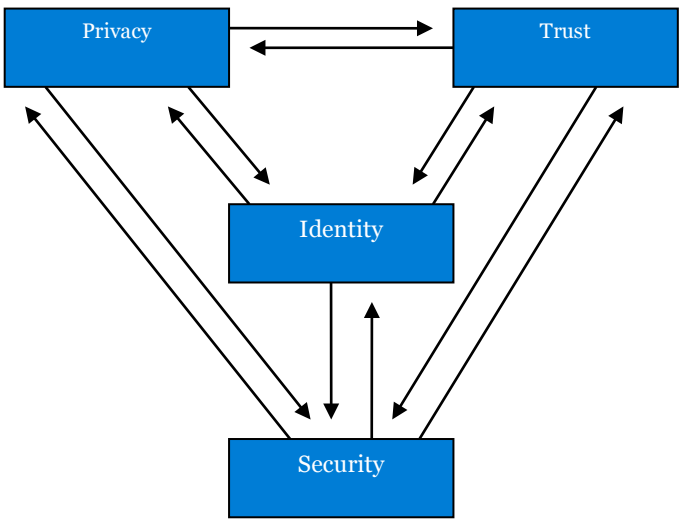


Figure 2 Related IDMS disciplines and their interactions

Privacy and trust form another part of the complex interaction. IDMS involve the collection, storage, and use of personal information; it is this aspect of IDMS that can raise concerns, as systems may be collecting irrelevant information, which may be sensitive in nature and potentially impinge on an individual's *"right to be left alone"* (Warren & Brandeis, 1890). This is also where trust issues also come into play, mediating for the *uncertainty* created when collecting and using personal information (Riegelsberger, Sasse, & Mccarthy, 2005). Therefore, building up trust may alleviate the privacy concerns raised when dealing with identity.

However, interactions between identity, privacy, trust, and security are more complex than that which is has been alluded to above; all these concepts interact with each other in highly unpredictable ways. The kind of identity information being collected and used will have an impact on the security mechanisms that are required to protect it. The security systems implemented will determine the protection offered on the information collected, hence potentially affecting the level of privacy concerns. The amount of privacy offered will affect the trust subjects have in the system.

Furthermore, while security determines actual privacy levels, it might have little impact on individuals' privacy perceptions, which may be affected by the amount and type of personal information required. Privacy perception is also driven by trusting behaviour, which again might shift with regards to the identity information; for example our study in Chapter 6 found that *information quality* affects individuals' *system judgement* on the effectiveness of the IDMS in helping the organisation to fulfil its goals (see Section6.3.2). All the elements are tightly wound together, each dependent on the other. It is this constant ebb and flow of the elements in an IDMS and their emergent properties that make it difficult to balance, and hence problematic to design and implement.

1.5.1 Limitations of Current Approaches

A review of published literature shows that research into the non-technical aspects of IDMS largely focuses on privacy and trust. However, these approaches are insufficient to understanding all the human factors involved, failing to link concerns directly to the concept of identity (Rahaman & Sasse, 2011). Most research in the privacy and trust field view identity as a peripheral component to the investigation thus, leading to an incomplete representation of identity concerns.

1.5.1.1 Privacy research

Privacy is a multi-dimensional concept, and as such there are various interpretations of its meaning. However, looking at the nature of IDMS and its information collection practices, privacy research tends to focus on the issue of *information privacy* (Smith, Milberg, & Burke, 1996). This form of privacy focuses on the concerns that people may have involving the collection of personal information. Informational privacy studies are widely accepted in computer literature, and thus have a large empirical base for support.

However, when considering the reach of identity systems today, the information privacy boundary is no longer sustainable. Privacy is still a concern, but it moves from the points of specific informational details to include the broader outcomes that privacy breaches bring; it moves to the *"lived experience of identity"* (Rahaman & Sasse, 2011). Therefore, a more encompassing view of privacy is required to generate a full picture of concerns in regards to IDMS.

Furthermore, information privacy research results in theoretical 'human-centred' solutions in the forms of *Privacy Enhancing Technologies* (Section 3.2.4), as well as influencing the development of laws and rules that are centred on the concept of *confidentiality* (Section 3.2.3). These approaches typically tackle the area from an organisational perspective, with the aim of promoting business through the *"free and uninterrupted (but responsible) flow and uses of personal data"* (Cavoukian, 2009). This results in utilitarian models that typically empower organisations to collect a greater amount of personal information rather than specifically addressing the underlying privacy concerns related to identity.

1.5.1.2 Trust research

As with privacy, trust is a multi-facetted concept, and its definition varies between different research disciplines. In the *Theory of Planned Behaviour* and the *Theory of Reasoned Action*, a model was developed with elements that can be used to predict behaviour (Ajzen, 1991; Fishbein & Ajzen, 1975). These models of behaviour have been used to develop several trust models that are currently used to assess trusting intentions in relation to e-Government and e-Commerce contexts (Carter & Bélanger, 2005; Davis, 1985; McKnight, Choudhury, & Kacmar, 2002a; Venkatesh & Davis, 2010).

These models of trust have proliferated in the computer science literature, especially in e-Commerce. However, the trust models do not identify how trust is shaped by the design of the system itself; the main focus is the generation of trust through general *attitudes* and *beliefs*, rather than the specific design issues that trigger trust concerns in the first place (Rahaman & Sasse, 2011). In order to implement more trustworthy identity systems, an understanding about how IDMS design can influence individuals' trusting intentions is required.

1.5.1.3 Organisational research

While privacy and trust cover individual perspectives of IDMS, the organisation implementing the identity system is also an important consideration. It is the organisation that determines the eventual design of the system, and therefore its implications for individuals. Furthermore, approaching organisations as large network of *"Human Activity Systems"* (Checkland & Scholes, 1990) adds further relevance of organisational research when taking a human centred approach to identity.

Unfortunately, there is little evidence in the literature of this approach being taken. While Kubicek & Noack (2010a) detail a framework outlining an actor-centred political process that leads to the form and structure of upgraded N-IDMS in Europe, other common organisational approaches tend to focus on identity as a mechanism with which to access resources (for an example, see White, 2008). These views are too limited because identity is no longer just a medium with which to access information, but an item of strategic interest itself; examples range from using identity in the backend for personalised advertising (see Phorm in Section 5.3.3), to identifying terrorists (see UK N-IDMS in Section 7.2.2), as well as using a child database to predict future criminals (see Contactpoint in Section 2.3.4.2). Research needs to accommodate this growing importance of identity within organisations.

1.6 Research Question and Aims

The research presented in this thesis seeks to go beyond the traditional perspectives of trust, privacy, and organisational paradigms. This thesis approaches the problem situation by investigating the core component of IDMS; i.e. the identity itself. With this in mind, the overarching research question can be surmised as:

What are the human factors that influence identity, and how does it affect the development, implementation and use of Identity Management Systems?

This thesis seeks to develop a holistic understanding of the how people relate to an IDMS. Therefore, guided by the overall research question, this thesis aims to:

1. **Identify the relationship between the individual and the IDMS.**
    a. How does the implementation design of the IDMS affect the lived experience?
    b. How does an individual perceive and make judgements about an IDMS?
2. **Identify the relationship between the organisation and the IDMS.**
    a. What are the organisations identity requirements?
    b. What factors affect the organisations design of an IDMS?
3. **To identify and develop a framework for the overall relationship between the individual, the system and the implementing organisation.**

1.6.1 Research Scope

This thesis is focused on developing a better understanding of human-centred IDMS; it is a substantive contribution, and does not seek to develop a new identity system or specific technology. The emphasis of this research is on the individuals and organisations involved in the development and use of an IDMS, and not on the detailed security or technical aspects of the system.

Furtherore, the scope of this research is limited to that of national government implementations. The government of Brunei Darussalam sponsored the PhD grant; their main interest lies in the development of countrywide systems, and this thesis aimed to provide knowledge on how an effective and acceptable N-IDMS can be developed. However, the results of the thesis are believed to be generalizable to non-government IDMS, and this thesis briefly explores the applicability of some the findings in these scenarios (see Section 5.3.1).

1.7 Research Approach

The phenomenon under investigation takes place in a complex socio-technical space. Current claims of 'human-centred' IDMS are largely rhetoric, and are based on assumptions and ideas that have not been tested in practice. Therefore, the research takes on an exploratory nature - it approaches identity from a new perspective, and that has not been explored in the available literature. The aim of the research presented in this thesis is to develop a new descriptive theory that captures the impact of system design on individuals' lived_experience, individuals' perceptions of an IDMS, as well as organisations' strategic considerations when implementing an identity system.

Based on the aims of this thesis, the research is broken down into three different studies:

1. **System Study.** This research investigates how the design of an IDMS may influence the lived experience of individuals.
2. **Individual study.** This phase of the research investigates individuals' perceptions of identity systems. The intention of the work is to uncover how individuals assess IDMS, and how it may eventually determine his/her willingness to accept an IDMS.
3. **Organisation study.** Finally, the thesis investigates organisational needs in the process of developing and implementing an IDMS. Viewing identity as a strategic resource, this research explores the relationships between the organisation's identity requirements, and the system design.

The main contribution of this thesis is an in-depth narrative of the identity situation, integrating 3 different but related perspectives. Bringing together the frameworks developed in the system, individual, and organisation studies, this research produced a unified framework that outlines the human factors that influence the development, implementation, and use of IDMS.

1.7.1 Methodology

Given that the focus of the investigation is on exploration and discovery, the research here utilised qualitative methods to develop a theory that emerges from the data. *Grounded Theory* (Charmaz, 2006; Corbin & Strauss, 1990; Punch, 1998) analysis techniques were applied throughout the thesis, while data collection methods varied between each study.

The system study used *Historiography* (Berg, 2001) to identify secondary sources of information that outline various past and present implementations of N-IDMS, and the corresponding outcomes. Research on the individual perspective made use of focus groups in order to elicit discussions and uncover individual concerns when encountering N-IDMS. Finally, the government study analysed interviews and official government documents to uncover organisational considerations when planning and running an identity system.

The organisation study used a case study research design; three different countries were identified for investigation, which covered diverse situations and constraints, while still maintaining comparability. The countries and systems identified are:

1. **Brunei.** The government of Brunei has been running an N-IDMS since 1949. It updated its infrastructure in 2000, when it implemented a multi-function smart card system. The identity systems have always been well received by the public, but its multi-function feature is currently under-utilised.
2. **United Kingdom.** The British government has had two short-lived experiences with N-IDMS in the past. A recent effort to implement a new system faced mass opposition, and has recently been scrapped. Government arguments for the new system generally fall under the branch of national security.
3. **India.** The government is currently in the process of implementing an N-IDMS. Little public opposition to the system has been identified. The government claims that its motive for implementation of an N-IDMS is the difficulties that the general public (especially the poor) face in proving their identity; individuals are thus are left without any access to required services.

1.8 Contributions

The major contributions of the thesis are:

1. **The development of a unified framework that captures a multi-stakeholder view of IDMS design and its implications. This includes:**

a. A set of *structural and metrical design properties* that in combination can be used to narrate the individuals' *lived experience* of identity
b. A framework that captures individuals' initial *perceptions* and willingness to accept IDMS, and how it is mediated by *system judgement, situation perception and security concerns*.
c. A framework that describes organisations *identity requirements* and how it influences the information and technologies chosen for implementation.

This is supported by several minor contributions, including:

2. **Guidance for practitioners to implement more effective human-centred IDMS:**
    a. To ensure that the system is fit-for-purpose, by designing the system according to organisations' identity requirements.
    b. The continuous engagement with all relying parties to elicit their goals and accessibility requirements, which need to be built into the IDMS.
    c. To look beyond the organisation, and include individuals into the design process, addressing individuals concerns, as well as ensuring that the lived experience created does not derail the purpose of the system.
    d. A method of possibly capturing the economic benefits for pursuing a human-centred IDMS design.
3. **The identification of potential areas of research:**
    a. The research presents a new approach to identity within HCI; researchers are encouraged to look beyond usability issues, and explore the lived experience.
    b. Privacy research could gain from moving beyond the informational privacy domain, to focus on an inclusion of the implications and consequences of privacy breaches.
    c. Trust research should investigate the effects that specific context and design of a system (as opposed to general attitude constructs) can have on individuals' intentions, and thus trusting intention.
    d. Research would also benefit from an exploration of culture and its effects on trusting behaviour.

1.8.1 Publications

The research conducted here has resulted in the publication of several papers. These are detailed in Table 2, along with the chapters that they correspond to.

Table 2 Papers published, and the chapters they correspond to

Publication	Chapter
Rahaman, A., & Sasse, M. 2010. *A framework for the lived experience of identity.* Identity in the Information Society. 3(3):605-638.	6
Rahaman, A., & Sasse, M. 2011. *Trust in national identity management systems: exploring citizen risk perceptions*. Presented at the IDTrust 2011 symposium, NIST, Gaithersburg	7
Rahaman, A., & Sasse, M. *Designing National Identity: an organisational perspective on the requirements for a National Identity System.* Submitted for publication to ICDS 2012.	8

1.9 Thesis Structure

Chapter 2 provides a review of 14 past and present IDMS implemented by governments. From medieval wanted lists to modern day eID systems, the chapter identifies the main catalysts and motives that drive the development of IDMS. The chapter also examines the effectiveness of each system, as well as overall outcomes of each implementation. In conclusion, the chapter draws several insights from the review:

1. The impact of identity and IDMS on behaviour
2. The influence of culture on perception of identity
3. The importance of a clear purpose
4. The setting of policies to support the purpose

Chapter 3 reviews the current research literature on identity, privacy and trust. Cultural studies are also reviewed, as well as the literature relating to organisations and N-IDMS. The chapter ends by identifying the limitations and gaps that this thesis will address:

1. A limited view of identity as an authentication mechanism, ignoring the growing use of identity as a strategic resource being accessed.
2. The focus on informational privacy and its confidentiality paradigm, forgoing the larger implications of identity and information on the lived experience.

3. The development of trusting intentions built on abstract trusting bases, thus not accounting for how the design of the system can influence risk perceptions.
4. A lack of published research on the impact of national culture on the willingness of individuals to accept IDMS.
5. Organisations tend to short-circuit identity debates, typically falling back on certainties of technologies, instead of ensuring systems that are fit-for-purpose.

Chapter 4 details the methodology used in the thesis. The research approaches the subject matter from different perspectives, each using different methods and data sources according to the line of investigation pursued.

Table 3 List of studies, and the respective methods used

Study	Data Source	Method of Analysis
System study	Historiography	Thematic Coding
Individual study	Focus Groups Survey data	Grounded theory Structural Equation Modelling
Organisation study	Interviews Publicly available documentation	Grounded theory

Chapter 5 details the first study conducted, i.e. the system study. Based on the systems reviewed in Chapter 2, the focus of this study is on identifying how system design can affect individuals' lived experience. The study produced a set of *structural* and *metrical* IDMS *design properties* that affect the *lived experience*; the *structural properties* focus on the flow of information within the identity ecosystem, while the *metrical properties* revolves around the qualities of the information that make up the identity.

Chapter 6 shifts attention onto individuals' perceptions of IDMS. Analysing data collected from focus groups, this study developed a framework that captured individuals' concerns when encountering new systems, and thus its effect on their intention to adopt. A survey based on these individuals' perceptions was developed and distributed. The results were then analysed and used to confirm and streamline this framework. The major constructs are:

1. **Situation perception**. Individuals' perceptions of the problem that the IDMS is supposed to address.
2. **Concerns. Individuals' concerns over the security of the identity within the system.**
3. **System Judgement.** Individuals' views on the effectiveness of the system in tackling the stated problem.

Chapter 7 presents the final study in this thesis, the organisation study. Analysing current implementations of N-IDMS in Brunei, UK, and India, the results of the study produced a framework that outlines organisations' identity requirements, and the factors that affect the eventual design of the IDMS. The framework highlights the importance of *purpose* in defining the organisations *identity requirements* over *identity creation* and *identity use***.**

Chapter 8 presents a synthesis of the three studies into a single *unified framework*. Going back to the data, relationships between the three frameworks are identified. Ultimately, the organisation's *purpose* and *requirements* will determine the *structural* and *metrical* design of the IDMS, which in turn will influence individuals' *perception*, and the eventual *lived experience*.

Chapter 9 details the verification of the research findings. Using expert evaluations of the unified framework, experts generally agree that the research being conducted is important, detailed, and overall useful to both practitioners and researchers

Chapter 10 provides a simple illustration of how organisations can use the framework to produce true human-centred IDMS. This chapter also examines the use of the framework constructs to determine the economic impacts of a human-centred system.

Chapter 11 concludes the thesis by outlining the contributions of the thesis that encourage researchers to move beyond traditional paradigms in the field. The practical implications for organisations' practices are also reviewed.

Chapter 2: History of N-IDMS

> *"Registration and documentation of individual identity are essential if persons are to count in a world increasingly distant from face-to-face encounters characteristic of less complex societies."* (Caplan & Torpey, 2001)

Many countries today are currently investing in their N-IDMS infrastructure, migrating from old paper-based systems to digitally based implementations. While investigations into current efforts may reveal a wealth of useful information, history itself can shed light on the state of identity today. Delving into the history of identification techniques and applications reveals a long evolving set of schemes that were implemented for various purposes and with a wide-ranging set of consequences; as Caplan & Torpey (2001) point out, *"the history of identifying practices has multiple origins and paths."*

The purpose of this chapter is to uncover, through the review of secondary data sources, the stated purpose of the IDMS, and comparing it to the recorded outcomes and public reaction thus determining areas of further research.

The following review is not limited to the notion of N-IDMS as ID cards for the whole population, but also covers other forms of government IDMS, such as passports and criminal systems. Further, the systems chosen for review (see Table 4) were selected to ensure that the review covered the major developments of government identity technologies in each of the themes uncovered; for example in the area of crime, this review followed the introduction of anthropometry, to dactyloscopy, as well as DNA. It should also be noted that the review was limited to the availability of secondary sources that could be used in the review; for example, language was a major barrier identified, limiting the sources of information to English based material.

The review takes a thematic approach, by first highlighting the evolution of administrative process, followed by a review of important historical concepts that led to the eventual implementation of government IDMS (see Section 2.2). This is then compared and contrasted to a review of current themes that are affecting systems today (see Section 2.3). Where relevant, strands of surveillance theory are introduced to promote a more complete and rounded understanding of identity and government. Additionally, details of past and present identification schemes are provided as examples of each theme.

2.1 Representation of Identity through Time

Identification is a dialectic process. It involves the transfer of information from one party to another; it is *"an assertion of a truth"* (Cameron, 2005). This implies the use of a common medium and language by which this claim to truth is made, i.e. the representation of the identity. There have been two major shifts that have affected the medium in which identification takes place; the first is the shift from oral practices to that of written forms of identity; the second, and currently on-going, is that of written identity to digital representations.

2.1.1 Evolution of Administration: Oral Memories to Written Proofs

One of the most prominent forces that have led to the development of N-IDMS is the establishment of formal modes of government administration; of particular interest are the mechanisms that support the functioning of bureaucratic processes. The centralisation of government administration, as well as its migration from the use of spoken language to that of written records, is one of the major historical turning points that began to shift weight onto the usefulness of an identity system (Groebner, 2001).

In England, the rise of literacy and its application in business began in the eleventh century. Clanchy (1979) illustrates the increasing dominance of written records during this period, by providing an account of the number of surviving records available today; documents dating back to the Anglo-Saxon era number about 2000, while records dating to 13th century England number in the tens of thousands. It was during this time that a shift from oral traditions based on memory to written documentation began to occur, the advantage of the latter being its ability to capture events.

The rule of King William during the 11th century is commonly considered a catalyst for the uses of documentation (Yates, 1966). Through the codification and compilation of law, reliance on documentation slowly began to take root. In prior oral customs, objects were commonly used to represent ownership. For example, a sword passed down through the generations might have represented ownership of land (Clanchy, 1979).

However, these symbolic objects were not very robust, as their meanings could easily be lost when dependent on verbal transmission (Clanchy, 1979). Soon, written charters replaced the old methods, as documents are more capable of preserving memory reliably over time. This in itself represented a form of identity, one that identifies the named individual as the owner of the land or object in question.

Soon, documentation, and hence written forms of identification, spread to all levels of community (Clanchy, 1979); government required the names of villagers in order to collect tax; individuals required testimonials of their trustworthiness to enter counties or villages, while other certificates of identity might offer a person entitlements or protection:

> *"Miles Earl of Hereford to all his friends, French and English, of England and of Wales, greeting. You are to know that this Folebarba is my jester and my man. So I entreat all my friends that they look after him, lest harm happen to him. And if anyone does him good for love of me, I will know how to thank him."* (John et al. 1964 in Clanchy, 1979)

As this brief discussion has illustrated, the evolution of oral memories to written administration triggered a change in identifying practices. Names came to be recorded in writing, charters to represent ownership, and certificates as testimonials of trust and warrants of identity. Slowly, the use of written documents was eventually 'perfected' and elevated to its modern incarnation that we are familiar with today (e.g. passports, birth certificates). The introduction of new identifying techniques over the ages was in part driven by the need to keep identity practices up to date with administrative processes and ambitions.

2.1.2 From Analogue to Digital

Eventually, technology was employed in service of this written structure of administration. However, as interactions in society have remained relatively unchanged (i.e. they are still dominated by face-to-face communication), the use of technology has always been that of a support mechanism for the written practices. This is no longer the case as today's advancement opens new corridors of communication and interaction.

On the premise of greater efficiency and productivity, governments are embracing technology (Layne & Lee, 2001), and in the process are progressing from the analogue written records of the past towards the digitalisation of data and information. Thus, the movement towards digital administration will bring with it a shift from written to digital identity.

Many governments have already begun to make use of digital identity documents, such as passports. Recent passport standards published by the International Civil Aviation Organisation (ICAO) have spurred several countries to introduce passports that include digital fingerprints and photographs. In the wake of this, countries have begun to place restrictions on non-digital passports in the form of visa requirements that typically capture the required information in machine-readable form. Already, certain privileges are being taken away from those who do not hold a digital form of identity; without a machine-readable passport or waiver, entry into a country can be denied.

Words on paper are no longer sufficient for today's governments as they begin to automate and interact through technology. In order to fully embrace and interact with the new digital administration, individuals need to be able to represent themselves in digital form. This is the shift that governments are now experiencing and, as a result, identifying practices are evolving along with it.

2.2 Historical Catalyst to Identity Systems

The current state of identity is built on the foundation of previous experiences in the field. A review of the literature in this area reveals that the present identity situation has been shaped by the need of service provision, the development of nation states, the increase in migration, and the problem of crime. The following provides an overview of these catalysts to past identity systems.

2.2.1 Service Provision: Benefit and Service Claim

Identity is a construct that connects an individual to a social order, and enables that individual to interact with other people and organisations; what an individual can and cannot do is dictated by who he/she is in a given society. Successfully assuming a false identity provides an imposter with access to all sorts of activities and resources that can be extracted from society (see Davis, 1983; Finlay, 1988, for detail of the 12-year impersontation of Martin Guerre, and how he was able to participate in society).

Table 4 List of IDMS reviewed, the main information collected, the identity record, the purpose, and outcomes

System	*Information Collected*	*Identity Record*	*Purpose*	*Outcome*
Poor Laws and Badges	*Group Affiliation*	*Tokens*	*Provide proof to licensed beggars*	*Poor refused to come forward, feeling shame, and to prevent their children from being taken away.*
Criminal Wanted Lists	*Clothes*	*Document*	*Identification of known criminals*	*Criminals evaded identification by using disguises.*
Russian Passports	*Residence*	*Document*	*Track and restrict movement of locals*	*Attempts to flee country.*
Passports	*Nationality*	*Document Database*	*To prevent or monitor the entry of dangerous foreign radicals into the country*	*Continued enrolment, to gain protection overseas.*
French Nomad Law	*Travel History Anthropometry*	*Document*	*Monitoring of unwanted members of the population*	*Abandonment of nomadic lifestyle.*
ID Cards UK (WW! and WWII)	*Nationality Photograph*	*Document*	*Rationing food to public*	*ID card schemes were rejected for their 'prussianizing' qualities.*
ID Cards UK (today)	*Nationality Photograph*	*Document Database*	*Aid in the fight against terrorism, crime, illegal migration, and benefit fraud*	*Protest by privacy groups.* *ID card scheme decommissioned in 2010.*
ID Cards Nazi Germany (WWII)	*Nationality Photograph*	*Document*	*To track and monitor individuals*	*Population was exposed to "paralyzing" surveillance.* *Aided in the genocide of Jewish population.*
ID Cards Germany (today)	*Nationality Photograph*	*Document Database*	*Support e-Government goals*	*Dangers of function creep and privacy invasions have been raised*

System	*Information Collected*	*Identity Record*	*Purpose*	*Outcome*
Schengen	*Nationality* *Photograph*	*Document* *Database*	*Stimulate freedom of movement within European Union*	*Free flow of movement between EU countries*
Bertillonage	*Anthropometry* *Photograph* *Verbal Portrait*	*Database*	*Identify recidivists for sentencing*	*Revolutionised criminal identification, but suffered from issues of subjectivity, and could not be used on women or children.* *In Argentina, public rejected the procedure which damaged 'honour'.*
Dactyloscopy	*Fingerprint*	*Database*	*Identify recidivists* *Forensic investigation*	*Warnings from experts about its fallibility, leading to the imprisonment of innocent*
US Visit Programme	*Fingerprint*	*Database*	*Identify criminals and terrorists entering or leaving the country*	*Drop in the number of visitors as people feel unwelcomed* *Retaliation by Brazilian government (US citizen fingerprints)*
UAE Iris Scan	*Iris*	*Database*	*Identify banned individuals from the country*	*High success rate in preventing re-entry of banned individuals*
Criminal DNA Database	*DNA*	*Database*	*Forensic investigation*	*Global controversy of such schemes, which is seen as a significant breach of privacy.*
Contact Point	*Contact history*	*Database*	*Protection children at risk, before harm is caused*	*Concern about government's ability to protect personal information.*
PKI and Digital Signatures	*Nationality*	*Document* *Database*	*Provide individuals access to online services*	*Limited adoption by the public.*

It is to this end that society attempts to bridge the gap of uncertainty that lies between the claimed identity and the true identity. The depth to which the identity mechanism attempts to close this gap is dependent on what is at stake. Taking an example from Camp (2004), money can serve as a loosely binding identification token; the money a person holds allows him or her to trade it in for a product or service of perceived equal value. In other situations, the entitlement to certain benefits may not be as loose, and it is in these situations where identification procedures are critical, as the identity is repeatedly called into question.

As the need for more accurate and verifiable representations arose, more robust identity procedures were developed, which involved more secure forms of registration, identification, authentication, and authorisation. In the process, the issue became drawn into bureaucratic forms of identity that enabled the growth of formal modes of government.

Drawing parallels with the field of surveillance studies, the rise of bureaucracy is theorised to inflate surveillance practices (Lyon, 2002). Surveillance activities are built on the files of information about individuals, which allow organisations to perform rationalised calculated actions. While the initial forms of identity do not represent a mature bureaucratic body, it did plant the seeds for such *officialdom*.

2.2.1.1 Ancient Egypt and the distribution of allowance

According to Ashbourn (2004), identity played a key role in the administration of food to the work force involved in the construction of the pyramids. To claim the entitled food allowance, each member of the workforce was required to present himself to the administrator in charge, state his identity verbally, and put forward his claim; food would be provided to an individual once the administrator was satisfied with the authenticity of an individual's claim. However, it was not unheard of for individuals to attempt to obtain the allowance more than once. An identity scheme was needed to prevent these false claims from proceeding.

With this in mind, an identity system was developed that made use of a mixture of various biographical and biometrical information. As each claimant came forward, unique physical characteristics as well as behaviour were noted and verified against written records. Where there were no outstanding features, the system resorted to the use of anthropometric measurements (bodily measurements). Food allowance was only provided once the identity had been fully verified, thus putting an end to the false claims.

2.2.1.2 Poor Laws, beggars and badges

Poverty in England had become a major problem towards the end of the 16th century (Carroll, 1996). The growth of the population and inflation were major contributors to the situation. With the poorest being hardest hit, many individuals turned to begging for survival. Early responses to aiding the poor typically came from monastery support and sermons that tapped into the religious beliefs to provide aid. The authorities eventually took over the responsibility for supporting the poor.

At this time, the authorities became concerned about the existence of *sturdy beggars* living among those who were genuinely poor (Carroll, 1996); these were fraudsters who preyed on charities by faking mutilation and disabilities. The authorities devised a system that licensed real beggars, and in doing so provided tokens that symbolised their right to beg and request for alms.

However, many individuals refused to obtain a license. According to Hindle (2004), beggars were required to wear the badges at all times, inducing feelings of shame. Furthermore, children within the households were also forced to wear the badge, and could be removed from their families. Thus, individuals chose to resort to crime, making the situation worse than it originally had been.

2.2.2 The Development of Nation States and Identification Practices

Other than service provision, the rise of nation states also had an impact on the identification practices of government. The enforcement of boundaries around a country and the attribution of individuals as belonging to a particular country only effectively came into being after World War II (Torpey, 2001). However, the late inception of nation states should not be mistaken as having only a small impact on the development of N-IDMS. The concept of rallying individuals to a particular cause, i.e. the country, creates a powerful mechanism that gives governments authority over individuals.

Prior to government involvement, identifying documents were provided by private entities such as churches, market organisations, and localities; these entities vouched for their members by providing documentation to ensure safe passage between geographically different places. In the Middle Ages, feudalism, serfdom, and slavery greatly supported this type of identity system (Torpey, 2000). During these times of social ordering and segregation, the lower classes of society were ruled and controlled by their masters; landlords governed over the serfs who worked the land, while slaves were under the control of slaveholders.

However, as nation states developed, governments came to play a constantly increasing role in shaping the future of the country and all its inhabitants. The ambiguous nature of these nation states, at once *"sheltering and dominating"*, require the capability to establish the identities of the people residing within them (Torpey, 2000); the dual natured policies sought to capture identity for the sake of securing resources (human or otherwise), as well as to establish control over individuals, for their own safety and that of the country (Torpey, 2000).

In attempting to embrace the population, governments began to take steps to retrieve control of the identification system. Early attempts made use of the available private infrastructure to keep tabs on the population. For example, France made use of parish registers to establish and recognise the civil identity of an individual (Noiriel & Laforcade, 1996). In Imperial Russia, metrical books (registers that held records of births, deaths and marriages) maintained by religious institutions remained the de facto identity mechanism until 1917 (Steinwedel, 2001). However, these situations typically led to the undesirable exclusion of certain religious groups.

Therefore, nation states created greater civic inclusion by reducing their dependence on third party identities. Nationality, and in some cases ethnicity, became the measure by which civil status was established. This created a more homogenous population in the eyes of the state despite the diversity of the public. The transformation produced *"the levelling of the governed",* and the establishment of direct relationships between government and individual, both of which are signs of a modern state (Steinwedel, 2001; Weber, Roth, & Wittich, 1978). Thus, the concept of nationality took centre stage, and citizens came to rely on the government to issue *official* identities, without which they would be lost within the society (Lips et al., 2005).

The field of surveillance studies has also touched on the role of nation states in the development of surveillance practices. In this field of research, surveillance is theorised to have arisen from military origins (Lyon, 2002). Citizenship rights are thought to be extended after wars, which concomitantly entail military surveillance measures. The military struggles led to the development of internal controls as nation states sought to embrace the local population, while protecting them from external harms.

2.2.2.1 Nazi Germany, Vichy France and national identity

Totalitarian regimes seek to establish strict control and order over society; exerting influence over every aspect of public life requires the regulation of individuals within the country. Typically built on the premise of nationalism and national rebirth, this emphasises the need on the part of the government to identify those who meet certain criteria that fits with the state's vision.

The government seeks to embrace the people it represents, while rejecting others who have no right to be there. Therefore, a totalitarian regime needs to develop rules and practices that ostracize problematic outsiders. Identification by nationality can form stronger bonds within society, while emphasising differences between target groups, thus drawing the public into the same thought pattern as that of the state. Those outside the group are made to be seen as a burden, and to possess a lower status.

Another important step is to establish a set of controls over the outsiders. In order to expose them to an increased level of surveillance, the government needs to establish a strong net of identifying procedures that discriminates against outsiders, controlling their movements, and in some cases criminalizing them or their practices. It is through state-issued national identity documentations that socialist and communist countries can gain control over their people (Werth, 2004).

Under the rule of the totalitarian Nazi party, Germany introduced an N-IDMS that provided the government with control over the movement of the native population, while exposing individuals to an unprecedented level of surveillance (Fussell, 2004). The government maintained various registers that gave law enforcement and intelligence officer's access to a wealth of information with which to carry out their task (Kempner, 1946). This level of surveillance allowed the state to quickly extinguish any signs of resistance while ensuring that everyone was working towards the government's vision.

The system was dependent on nationality and ethnicity, and served to *"deindividualize, dehumanize and demonize"* those whom the state considered to be un-worthy (Fussell, 2004). To this end, the government of Nazi Germany in 1938 began to mark the identity cards of Jews with a J-Stamp, enabling quick and easy identification; this eventually led to more visual forms of identification such as branding. This identity system separated the Jews from the rest of the population, allowing them to be constantly watched. It was also used as an aid in the genocide of the Jews and other minority groups residing in the German empire.

This comprehensive identity system was installed in the various countries Germany occupied, such as Poland, Norway and France, among others. Again here the J-Stamp was applied to the Jewish population, aiding in the genocide that took place (Fussell, 2004). In Norway alone, 750000 Jews were identified and sent to the death camps. Following the defeat of France by Germany, the Vichy regime established the French identity system and card in 1940. The *carte d'identité de Français*, as it was known, was also used in the identification of Jews. In this case, up to 76000 people were deported to death camps.

2.2.2.2 Great Britain, identity cards and World War I and II

Britain's first experience with an N-IDMS was in World War I, when a National Register was quickly passed through parliament for the purpose of recording all persons between the age of 15 and 65 (Agar, 2001). While there was great debate as to the possible intention on the part of the government to use the system for conscription (Agar, 2001; Elliot, 2006), the implementation was eventually agreed upon, if only to establish the number of men who would be capable to take arms in times of need. Once the required statistics were generated, interest in the system waned and it was eventually abandoned.

However, civil servants saw the potential value that such a system could offer during peaceful times, and set out guidelines that would ensure the continued relevance of an N-IDMS in times of calm. The government's strategy was to provide the identity system a *"parasitic value"* (Public Record Office 1923 in Agar, 2001) in such a way that it penetrated and attached itself to the activities of normal civilian life. The government found an opportunity to create such a system during World War II.

The administration believed that tying the system to food rationing would ensure the survival of an identity system (Institute for Public Policy Research, 1995). The requirement to produce identity cards to receive necessary supplies would motivate the public to keep hold of the card. This parasitic component helped to secure the relevance of the identity system well after the end of World War II. However, since food rationing could not serve to maintain public cooperation forever, the government attempted to attach the national register to the provision of health services (Agar, 2001; Flaherty, 1979).

Eventually, much opposition arose to the identity card as the public and media began to rally against the government. The Wilcock case proved to be the beginning of the end for the identity cards, in which John Wilcock refused to produce his identity card when randomly stopped by officers (Agar, 2005). The media and public viewed the system as *prussianizing*, and requests of identification by police unacceptable. The case was brought to court where the judged sided with Wilcock. The N-IDMS was decommissioned shortly after.

2.2.3 Migration

Nations are *imagined communities*, in which memberships are territorial in nature (B. Anderson, 1991). As modern states began to take shape, governments began to assume greater control over the movements of people in their territory; this was necessary in assuring social and civil stability within the country.

The main tool in designating a trans-national *legible citizen* (Scott, 1998) is the passport. A passport allows an individual to establish his/her identity and nationality, thus providing the right to move and receive assistance from the government. More importantly, passports provide the government with a means to prevent or stimulate the departure of its citizens, to identify and control alien movement, as well as enabling surveillance of the population (Lucassen, 2001).

Internal passports (see 2.2.3.1), precursors to the current passport system, were typically issued in times of serfdom and slavery; they were distributed to control the movement of the lower classes within the country (Garcelon, 2001). These documents were eventually abolished as people were given their freedom, and as capitalism replaced feudalism, government thus recognised the value of mobile individuals (Torpey, 2001).

However, passport documentation soon reappeared in the early stages of the nineteenth century, during which the revolutionary climate posed a threat to many countries stability. Passport controls were introduced to identify and prevent the entry of dangerous aliens (Lucassen, 2001). Thus, new regulations were enforced on foreigners; they were required to possess a passport from their country of origin, as well as a visa issued by the country of entry.

Eventually, the political climate shifted towards a more liberal attitude with respect to the movement of people. Again, as with internal passports, influence came from economic liberalism; suspicions towards foreigners were replaced by the recognition of potential value (Torpey, 2001). It was during this period that Europe saw the abolition of passport and visa obligations as the region entered a period of identity *lassiez faire* (Lucassen, 2001; Noiriel & Laforcade, 1996).

However, this open-door policy on movement came to an end during World War I. Identity requirements that had been loosened before were now reinforced, and were stronger than ever. For example, passports were not only required to enter Germany, but also required by those wishing to leave the empire (Torpey, 2001). Therefore, with a revised purpose, the new identification documents were not only enforced on immigrants but also the entire local population. Unlike previous passport controls, these policies continued to remain in effect after the war, as states were faced with other burdens, such as welfare provision, during peacetime.

After World War I, states assumed greater responsibility in the economic domain (Lucassen, 2001). The development of welfare states is one of the reasons why the rigid document controls on identity and movement remained (Lucassen, 1998). Armed with an interest in the socioeconomic welfare of the people, countries were concerned about the influx of poor immigrants. To protect the local work force, passport controls were used to regulate the entrance of aliens into the national labour markets. Additionally, identity records were important in distinguishing between nationals who had a right to aid from the government, and immigrants who were likely to be sent back home. Thus, the threats faced from migration spurred the need for tighter controls, and hence shaped passport documents to the form that we have become familiar with today.

Surveillance theories relating to the military struggles of a nation state are evident here. The development of the passport controls to prevent dangerous individuals from entering countries elucidated here can be related to efforts in obtaining information about enemies (Lyon, 2002). Theories surrounding the *political economy stream* of surveillance practices are also visible, where surveillance is carried out to enforce the interest of one class of people over another. While typically applied to surveillance in the private sectors, it is still relevant here. The capitalistic grounds of the political economy, and the sorting of consumers (i.e. the differentiation between nationals and non-nationals) are present in the development of welfare states.

2.2.3.1 Russian internal passport system

Serfdom in Russia was only abolished in 1861. Up to this time, peasants were subject to a multitude of laws that reinforced the feudalistic social order (Matthews, 1993). The government required mechanisms that would enable it to control and extract wealth from the country's largely serf population. The 1649 code of laws enacted local registers that tied peasants to a given estate. Under this law, anyone who was caught leaving the assigned land would be sent back (Eltis, 2002).

However, faced with the continuing prospect of serfs reneging on their obligations (paying tax, serving in the army, etc.), Peter the Great introduced internal passports (Matthews, 1993). Anyone who was travelling needed to be in possession of travel documents to be presented at police posts for inspection; serfs required written permission from the landowner, stating the intended destination and the duration of travel. Coupled with the high price in acquiring these passports, the identity system effectively removed serfs' right to movement.

The actual success of this system is difficult to assess, and records show that a large number of manhunts were launched to find individuals who evaded the system due to the extreme demands of the law (Matthews, 1993). The abolition of serfdom in 1861 did provide some individuals with freedom, but did not see the removal of internal passport controls. A relaxation of rules only occurred towards the end of the 19th century, as governments attempted to stimulate economic growth by mobilizing work forces (Eltis, 2002).

2.2.3.2 Dutch passport system 1813 - 1860

The French revolution under Napoleon came to an end in 1813. However, the instability that was still present in France after its defeat was considered to be a threat, and it became necessary to cordon this off with strong states. The Dutch Kingdom was formed through this need, and the implementation of the Dutch passport system was designed to monitor, control and prevent the influx of revolutionists and their ideas (Lucassen, 2001).

Under this system, any aliens entering the country were required to be in possession of a passport. The government's practices in selectively enforcing the system illustrated that this was a tool designed to target a particular population; French citizens experienced the full force of the passport measures and controls, while British nationals were treated much more leniently. The British government at the time did not issue passports to its citizens, yet the Dutch admitted British citizens into the country (Lucassen, 2001).

The revolutionary climate slowly dissipated in the mid-nineteenth century. This also coincided with the economic liberalization in the European region. With the French no longer being considered a threat to society, the emphasis was now on the potential value of immigrants (Torpey, 2001). Therefore, as it was no longer in the government's interest to stop movement of people, the passport requirements were abolished in the 1860s. However, records show that many people continued to enrol and make use of the passport system despite its abolition, as the passports allowed them to access protection and services within foreign countries (Lucassen, 2001).

2.2.3.3 French nomad law

In the early 20th century, the French began to show an increasingly negative attitude towards the nomadic population within the country. Public disapproval hit lows when people began to stereotype gypsies, associating them with socially unacceptable behaviour. The French government sought to control the situation by introducing methods that confined the movement of the nomads. It was hoped in this way to eliminate the gypsies through social integration (Kaluszynski, 2001).

The French Nomad Law of 1912 was developed for this purpose. The discriminatory nature of the law is revealed in the different categories of nomads that were posited. Despite the fact that travelling showmen shared the same mobility as gypsies, the showmen faced reduced obligations and penalties. For example, travelling showmen were only required to have an occupational identity card when travelling. Gypsies, on the other hand, were to obtain anthropometric identity passes that recorded physical characteristics (to capture their criminal otherness) of all members in the travelling group (Kaluszynski, 2001).

Gypsies were required to present these anthropometric passes to local law officials on arrival or departure from a community. Failure to abide by the law was met with severe fines and punishment. This was particularly problematic as local officials were given the authority to allow or disallow anyone to camp within their commune. The pass represented a powerful instrument of control to the government.

Fuelled by public distrust towards gypsies, the law remained in effect for over 20 years. In this time, the identity system was used successfully in persuading part of the gypsy population to give up their nomadic lifestyle. However, others who continued their lifestyle began to move more frequently due to the new restrictions (Kaluszynski, 2001).

2.2.4 Crime and Law Enforcement

Crime has always been a major catalyst in the development of identification techniques. Throughout medieval Europe, criminal identification mainly involved the use of physical descriptions to aid in the capture of criminals (see 2.2.4.1); tactics for subsequent identification of known criminals include the use of branding, which, while cheap and effective, posed problems for social integration (Cole, 2001). Specifically, the visibility and irreversibility of the method prevented criminals from being integrated into society. For example, branding was abandoned in England because *"it had not had its desired effect by deterring offenders from the further committing of crimes and offences, but on the contrary, such offenders, being rendered thereby unfit to be entrusted in any service or employment to get their livelihood in any honest or lawful way"* (Pike 1873, in Braithwaite, 1989).

While the abolition of branding was a success for human rights, it created problematic situations for law enforcement. With no effective means to re-identify criminals, authorities were faced with problems of recidivism (Kaluszynski, 2001). Where first offenders were to be rehabilitated and reintegrated into society, re-offenders were to be severely punished, and perhaps even segregated from the rest of society. The removal of branding gave first offenders better chances of social reintegration, but created problems in identifying recidivists who should have been given harsher punishments.

Some studies have attempted to use physical indicators to identify an individual as a criminal; it was assumed that criminals had a biological disposition to commit unlawful acts, and that this criminal nature would manifest itself physically (Cole, 2001; Gibson, 2002; Lombroso & Horton, 1911). In a way, this was a way of identifying group membership rather than specific identity. Suffice to say that this line of identification did not produce any valid results. Cole (2001) cites the example of all people with pointy-heads facing the wrath of the law as a possible consequence of this type of thinking. As such, the authorities were in desperate need of methods that would allow them to identify individual recidivists.

It was with respect to this belief that bertillonage and dactyloscopy were developed and applied. While anthropometry achieved some initial success in law enforcement, its reliability was questioned as it necessarily involved subjective human judgements in the capture of identity (see 2.2.4.2). Eventually, Dactyloscopy trumped the anthropometric solution as it produced results in a more consistent and accurate fashion (see 2.2.4.3). Additionally, a shift in the focus of identification took place. Police responsibilities grew, from only having to identify recidivists to include the identification of criminals who were present at the scene of the crime. Dactyloscopy was crucial in allowing law enforcement officials to carry out this task.

2.2.4.1 Physical description of individuals

As individuals in the Middle Ages started moving around between various communes, the identification of particular persons became problematic; at the time, people were reliant on personal experiences with an individual to construct the relevant identity (Clanchy, 1979). Therefore, it was necessary to fill this gap in the identification of dangerous individuals, who would otherwise remain unknown, as he/she would move around between different communities.

In the early medieval period, portraits and descriptions were used to fill this identification gap (Groebner, 2001). Typical of these early times were the distribution of criminal *wanted lists* to various communes in the hopes of revealing the true identity of the individual to the rest of society and also aiding law enforcement. The system was a mixed success as criminals devised techniques to counter the identification procedures. Early implementations made use of attire as the main descriptors, as clothes were expensive and difficult to come by. However, this meant that such individuals could evade identification by obtaining new clothes or donning disguises (Groebner, 1999).

2.2.4.2 France, recidivism and Bertillonage

Held in the grip of crime and recidivism, the authorities of 19th century France required a means of recognising repeat criminals so as to apply harsher punishments (Gibson, 2002). At the time, the police used photographs to identify criminals who had been previously arrested. As these photographs were stored and sorted by name, criminals easily circumvented detection by providing a false name. Recognising this, Alphonse Bertillon set out to create a criminal identification system based on a scientific verification of identity (Kaluszynski, 2001).

The resulting system, bertillonage, made use of a tripartite system; capturing the identity of a criminal resulted in a Bertillon card that contained 11 anthropometric measurements (i.e. scientific measurements of the human body), physical descriptions, and photographs (Cole, 2001). The main advantage of the Bertillon system came from the anthropometric measurements that were used in the filling system. Sorting through records now involved the precise matching of an individual's bodily measurements, which he/she could not lie about (Kaluszynski, 2001). The system revolutionised the field of criminal identification field, and was eventually implemented in several other countries.

However, Bertillonage was eventually abandoned, as it was incredibly complicated to take anthropometric measurements, requiring expensive precision equipment, and extensive training (Kaluszynski, 2001). Yet measurements and descriptions still contained subjective elements, such as descriptions of the eyes or in the estimating measurements. Furthermore, criminals could force errors in measurements through movement, such as the bending of the back or the arching of the foot (Joseph, 2001). The system was not applicable to women (due to physiological changes such as pregnancy), and children (who have yet to mature, and hence were still growing).

Bertillonage also face much opposition in Argentina, as the recording of measurements was seen as an attack on an individual's *honour*, which is described as *"the highest level of the human personality"* (Ruggiero, 2001). Resistance against the system was so strong that the identity records were regularly destroyed, even the records of criminals who had completed their sentence. This completely undermined the aim of the system to identify recidivists.

2.2.4.3 Forensics, criminal investigation and Dactyloscopy

The Bertillonage system of identification was short lived; the advantage of the filing system, and therefore the effectiveness of the identification process, soon appeared in other identification technologies. Dactyloscopy, a fingerprinting method, stored and retrieved identity records in a more logical and economical manner (Ruggiero, 2001). Dactyloscopy also reduced the subjectivity involved in the capture of the identity; the use of ink and paper to create *rolled fingerprints*, which *"presented a literal physical trace of the body"*, and provided the system with a perceived *mechanical objectivity* (Cole, 2001; Daston & Galison, 1992; Finn, 2005).

However, the true advantage of dactyloscopy lay in its forensic ability, extending its potential uses beyond those of Bertillonage; dactyloscopy not only allowed for positive identification of recidivists, but also provided authorities with forensic evidence that tied individuals to crime scenes.

The first recorded case of the forensic use of fingerprints came from Argentina in 1892 (Lee & Gaensslen, 1991). The local dactyloscopy advocate, Vucetich, was able to link a bloody fingerprint of Francisa Rojas to the crime scene of her murdered children. She eventually pleaded guilty under the weight of the evidence (Ruggiero, 2001). In 1898, the East India Company used dactyloscopy in a murder case investigation; the judge here deemed the evidence as enough to charge the party for trespassing and burglary, but claimed that the presence of the fingerprint was not proof of (Cole, 2001).

While fingerprint identification is still practiced widely today, recent studies have shown that fingerprint identification is not as infallible as most people believe it to be. A high error rate is prominent among practitioners comparing fingerprints, especially those retrieved from crime scenes. These errors have been found to result in the imprisonment of innocent individuals (Cole, 2004).

Investigating the murder of Marion Ross in 1997, the Scottish law authorities found fingerprint evidence that linked one Mr Asbury to the crime; this was eventually used in court where he was found guilty. More importantly, investigations also found fingerprints in the home that belonged to one Shirley McKie, who at the time was an officer on the case (BBC, 2000a). McKie maintained that she did not enter the victim's house, and so could not have left the fingerprint; if this were true, it would call into question the evidence against Asbury. Following this McKie was suspended, fired, and charged with perjury. Although McKie was acquitted two years later, it took her to 9 years in court actually get compensation in 2006, where the authorities still maintained that no error was made. A formal public inquiry was completed in 2011 which dismissed conspiracy issues that were raised throughout the ordeal as *"misidentifications due to weaknesses in the methodology"* (Campbell, 2011) ; 4 fingerprint experts working for the Scottish authorities all made positive identifications of McKie's fingerprints, while external experts claimed that it wasn't.

In the case of the 2004 Madrid bombings, FBI detained Brandon Mayfield on the account that his fingerprints matched those found at the scene; *"a 100% verified"* match (Isikoff & Pape, 2004; Murr, 2004). As a result, Mayfield spent 17 days in detention until Spanish law enforcement forced the FBI to admit its mistake, as the Spanish investigators matched the fingerprints to the true perpetrator.

2.3 Modern Parallels to Historical Contexts

Identity systems are continuously evolving; parallels can be drawn between the historical influences on identity and the current forces that shape today's systems. The developments in administrative procedures, the creation of virtual borders, as well as the emphasis on crime prevention and human rights can be traced back to the historical roots reviewed above. The following provides an overview of current themes.

2.3.1 e-Government and Virtual Borders

Identity has always been important in the provision of benefits and services (see 2.2.1). However, citizens of today are more mobile than ever before and have become dependent on the modern forms of communication to gain access to information and services. One of the goals of e-Government is the provision of services through the Internet. This new emphasis on online services requires new mechanisms for the identification of individuals; in order to operate in this digital medium, individuals need the ability to adequately represent themselves in the digital world.

A digital identity is required; one that will empower individuals, allowing them to assert their identity in a virtual environment, thus enabling them to access and claim services to which they have a right.

Taylor, Lips, & Organ (2006) have gone a step further, highlighting the similarity between the digital paradigm of e-Government and the historical use of identity documents in controlling access to countries' borders. Where the paper controls in the analogue world allowed individuals to enter and leave the country, a digital identity allows a government to restrict access within a digital setting. The equivalent of border checks would be the log in mechanisms required to access websites and online services. In this way, digital mechanisms control access to virtual territories, extending the government borders beyond the physical realm of a country's boundaries.

From a surveillance theory perspective, the shift in government administration and identification practices stems from the disembodiment of everyday interactions (Lyon, 2002). The earlier shift from oral to written records was the first act that contributed to the disappearing of bodies that allowed interactions to transcend space and time (see 2.1.1). The electronic medium allows individuals to further leap past these boundaries. Organisations therefore capture digital identities to extend their range and surveillance in order to establish and confirm their relationship to individuals who are not present.

2.3.1.1 The Belgian eID

The roll out of the Belgian eID scheme to nine million individuals began in 2004 (London School of Economics, 2005) . Replacing the previous paper-based system in place since 1919, the main focus of the new shift was to provide citizens with a secure channel through which to perform online transactions (Cock, Wouters, & Preneel, 2004) . The government also believes that the new platform, with added security, is essential in providing a more open, transparent and responsive administration (Cock et al., 2004). In order to fulfil these goals, the eID system made use of digital certificates in their identity cards, making Belgium the first country in Europe to do so (Cock, Wolf, & Preneel, 2006).

Comparing the eID implementation to the previous paper-based mechanism reveals that the information being collected remains unchanged, while the data stored on the chip reflects the data that lies on the face of the card, with the added digital signatures to support the new online environments. All the data being collected is stored in a central registry, as has been the case since 1919. Additionally, individuals are given the choice to opt out of the digital signing scheme.

Statistics on the actual usage of the eID for online services are scarce. A recent study has revealed that 44% of the working population has made use of eID from home (Grommen, 2009; Indigov, 2009; De Morgan, 2009). The study also states that there is limited adoption of the card in the workplace, while the digital signature capabilities are very rarely used at all (Mariën & Audenhove, 2010). Lack of e-readers at work is argued to be a main factor, with only an estimated 18.8% of all workers having access to the devices. Complexity of the software required and the lack of awareness on the uses of the eID, such as the validity of the digital signatures, were also highlighted as possible reasons for the poor rate of adoption.

2.3.1.2 Austrian Citizen Card

Austria is one of the forerunners of e-government in Europe. To facilitate its vision for the provision of online services, the government needed a system that would support citizen identification and interaction of services in a digital environment. The concept of the Austrian Citizen Card was defined to fill this role (Leitold & Posch, 2004).

The Citizen Card, contrary to its name, is not a single physical card. It is in fact a set of ideas, standards, and requirements that have been developed to support digital identification and authentication (Arora, 2008); it outlines mechanisms for secure identification numbers and digital signatures. To protect privacy, separate identity numbers are generated for each sector that an individual interacts with; there are 26 sectors in total (tax, health, education, etc.), each of which uses a different identifier per individual.

By focusing on the high level details instead of specific technology implementations, the government has created a highly flexible and inter-operable platform. Individuals can obtain Citizen Cards from a number of providers, and choose to load them onto various devices that include official government eCards, Bank ATM cards, and even mobile phones (Arora, 2008). The Austrian model is often highly regarded, and is seen as a benchmark for other countries intending to implement digital identification procedures.

However, recent studies have shown a low rate of adoption; by early 2009, only 74,000 individuals had activated their digital identities and signatures (Martens, 2010). This represents 0.9% of the overall Austrian population, a very slight increase of about 0.2% from the year ending 2005 (Meints & Hansen, 2006). A-Trust, an Austrian certification service provider, attributes the lack of adoption to the complexity, cost and lack of benefit from an individual's point of view (Sokolov, 2006a, 2006b).

2.3.2 Digital Nations

The development of nation states was a crucial turning point in the development of modern identity infrastructure. Based on law of the soil or law of the blood (Lips et al., 2005) that designates people according to the land of their birth or heritage, nationality forms an important part of a person's identity today. Without such a government-sanctioned identity, life for a citizen can be quite difficult. Access to benefits, privileges and protection is severely limited; in this way, governments establish authority over their people.

According to Lips et al. (2005), the universal access of services by citizens may be at risk from the technological developments happening in the realm of identity. The creation and use of digital identity may lead to a new law of information that presides over the status of citizenship. Technological developments, coupled with the wide availability of citizen information, give governments the ability to sort citizens, enabling segmentation in the provision of service (Lyon, 2007), effectively altering the relationship between citizen and the state (Lips et al., 2005).

In the past, attempts to establish authority over the entire population required that governments broke free from the private institutions that controlled identity (Steinwedel, 2001). This created a homogenous population in the eyes of the government. The population of today is now at risk of being segregated again; now this will be based on the information that can be linked to each individual, rather than attributes such as religious affiliation.

This fragmentation of society further echoes the bureaucratic theories of surveillance, where organisations seek to carry out rational calculable actions (Lyon, 2002). Identity and information provide governments with this rationalising ability, splitting the population into different groups on the basis of their digital persona, and hence attempting to predict the needs of individuals on the basis of group membership.

2.3.2.1 UK identity card scheme

The British government has recently scrapped its attempt to re-introduce an N-IDMS (BBC, 2008a). As with the insecurity of World War I and II justifying the need for such cards in the past, the latest push for an N-IDMS was driven by security issues such as terrorism, organised crime, illegal immigration, and benefit fraud.

In reviewing the scheme, Agar (2005) claims that the plan for the new N-IDMS had little *parasitic* value that would ensure the usefulness of the system during periods of calm. However, the possibility for the system to penetrate the various avenues of everyday life is realised when analysing the number of issues that the system is supposed to tackle. Function creep was one of the major arguments that privacy advocates raised in opposition to the implementation (London School of Economics, 2005). This danger is very real, and begins when the identity is requested by a large number of organisations. The N-IDMS would become a vital part of the country's infrastructure, seeping into the daily activities of everyday life. It is this function creep that, if unchecked, will provide the system its parasitic value, thus ensuring that life without it could come to a halt.

The plan to introduce a new N-IDMS has faced mass opposition from privacy advocates, as well as resistance from the general public. With a recent change in government, the current coalition party has scrapped plans for the system (BBC, 2010a).

2.3.2.2 German eID and the legacy of a totalitarian past

While the totalitarian Nazi regime was eventually defeated, its downfall did not bring with it the complete abolition of the identity system. German laws forbid the government from creating a central system to store biometric information (London School of Economics, 2005). Information is stored at local registration offices, and then destroyed once an identity card is produced. The system does not assign unique identity numbers to its citizens, nor can the serial numbers of identity cards be used as an identifier (Kubicek & Noack, 2010b). This prevents the potential function creep of the information, reducing chances of it being abused.

Another step that has been taken to prevent potential abuse of the system is the removal of group affiliation. The current German N-IDMS does not collect or store any information dealing with race or religion. This precaution can also be seen in other countries, especially in Europe. Fussell (2004) has noted that other countries are taking steps to abolish group classification in their national identity systems, including Greece, Georgia, Indonesia and Russia, among others.

Current efforts in the country are focused on the introduction of digital identity cards that make use of RFID chips and that can facilitate online transactions. The system will make use of pseudonyms that will be uniquely generated per card, per service (Banse, 2008; Bender, 2008; Birch, 2009). This is similar to the Austrian approach in the use of sector specific identity numbers, providing a layer of security by preventing the tracking of individuals across different public and private spheres. A point of controversy in the planning of the system was the mandatory provision of fingerprints; after much debate, the final decision was to make fingerprinting an optional opt-in scheme as an aid for travel (Noack & Kubicek, 2010).

2.3.2.3 Greek ID cards

While Greece does not have a digital N-IDMS, its recent reduction of its information collection practices for its paper-based system is worth noting. The situation faced by the Greek government is unique when compared to experiences encountered in other countries, as the public backlash it experienced occurred for atypical reasons.

All citizens of Greece who are 14 years of age or older are required to report to the police station to register for a paper-based National Identity card (London School of Economics, 2005). Citizens are required to carry the cards at all times, and since the police have the power to demand the card for inspection, failure to do so could lead to detention until proof of identity has been established (Fontana, 2003). All data collected is stored in a centralised database under the control and protection of the police.

Traditionally, the process of enrolment in Greece requires the collection of a large amount of personal information, including an individual's fingerprints, spouse's name and religion. All this information is printed on the card face, including the unique identity number. In 1993 the government passed a ruling that citizens are no longer required to declare their religious beliefs. However, this move to reduce data collection and protect privacy was met with resistance; thousands of people came together to rally against the new ruling (BBC, 2000b). With 97% of the population being members of the Orthodox Church, the religious declaration is argued to be a symbol of pride and a dedication to their faith (LoBaido, 2000).

Despite resistance, the government proceeded to abolish religious affiliation from the system; this was done to prevent discrimination against the minority who are not of the same faith. Along with religion, the government has stopped collecting fingerprints, as well as information on spouses, profession and residential address (London School of Economics, 2005).

2.3.3 Globalization and Travel

The role of identity in migration today has been largely shaped by the events of World War I (Lucassen, 1998). However, recent economic developments have seen a relaxation of the tight controls on identity controls and movement of people. In Europe, for example, the Schengen agreement has abolished the need for border checks in the European region (see 2.3.3.1). This has allowed people from the participating countries to move freely across borders. Other efforts in a similar vein include Trusted Traveller programs that allow individuals to pass through immigration points easily (see 2.3.3.2). To a certain degree, this mirrors the freedom of movement between countries that was witnessed during the pre-World War I era.

In contrast to this freedom of movement, countries are also taking measures to prevent the entry of unwanted individuals, and controls are even stronger than they were in the past (see 2.2.3). Again, here governments impose limitations with the intention of protecting the local population. The UAE bans foreigners from re-entry if they break the law while in the country (see 2.3.3.2), while other countries expose travellers to high levels of security to prevent or track the entry and exit of potentially dangerous criminals and terrorists (see 2.3.3.4).

2.3.3.1 Schengen agreement

The European Union has been steadily working on increasing collaboration between countries within the region. Driven by political, economic and social concerns, agreements have been made to facilitate free movement between participating parties. Under the Schengen agreement, border checks between the countries would be eliminated, aiding in the development of large markets in a union of rich states (T. Bauer & Zimmermann, 1997). To date, 25 European nation states comply with the agreement, allowing individuals to travel between each country using only an identity card (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Norway, Iceland and Switzerland) (European Commission Home Affairs, 2010).

Citizens from Schengen countries are not required to carry passports within the Schengen zone. However, if needs be, the agreements allow for identity cards from each respective country to be used as a proof of identity. Entries of foreign nationals into the EU zone pass through border checks, and still face passport controls. Once through border control, freedom of movement within the Schengen zone is typically granted. Identification information about individuals and property relating to external border security and law enforcement is stored in the Schengen Information System that is shared between countries (Lettice, 2005).

2.3.3.2 UK – IRIS immigration system

At the original time of this writing in early 2010, the United Kingdom Border Agency had iris recognition systems at certain border checkpoints. However, an update as of January 2012, the Border Agency website states that *"all enrolment rooms in [the] 'IRIS scheme definition document' has been superseded - all enrolment rooms are currently closed"* (UK Border Agency, 2012). While the system is still working for those already enrolled, it may signal that the iris system may be decommissioned in favour for facial recognition, which is briefly discussed in this section.

The aim of the IRIS system was to provide timesaving and convenience to individuals who are exempt from immigration controls, visa holders, as well as frequent flyers to the UK. It is a voluntary scheme, and is offered free of charge to those who are eligible. The system is designed such that travellers present their iris at the gate, which is then checked against all iris pattern stored in a database in a one-to-many matching operation.

Individuals making use of the system have reported bad experiences when using the iris system. Reports indicate false rejection rates at the barriers of up to 3.57% (Biometric Technology Today, 2007).

The UK Border agency has also been testing the use of facial recognition systems since 2008, and has now installed the system in 10 different airports across the country. The system is open to all citizens of European Economic Area countries, who hold biometric passports; the system works by automatically comparing individuals face to that stored on the chip of the passport. Usage statistics and satisfaction rates are currently unavailable; however an incident in February 2011 caused the border agency to suspend use of the machines for 3 days. A couple had been able to clear and walk through the automated the gates, despite having mistakenly swapped passports with one another; the issue was only spotted because an immigration officer was supervising the gates at the particular time (BBC, 2011b).

2.3.3.3 UAE - iris recognition

One of the recent challenges that the United Arab Emirates government faced was the re-entrance of expelled individuals into the country. Before the current system, border control relied on the use of biographical information for security; identification documents were crosschecked against a database of blacklisted individuals. However, deported individuals returned to the UAE with new passports containing altered information, thus allowing them to avoid detection (Rosenzwig, Kochems, & Schwartz, 2004).

The UAE government chose to make use of iris recognition as a means of overcoming the drawback of the previous system (Al-Raisi & Al-Khouri, 2008). Deployed in 2003, the system was designed such that there was a central database holding the iris patterns of all expelled individuals; 751 individuals as of 2006 (Al-Raisi & Al-Khouri, 2008). Entry borders were equipped with iris scanners that would cross check the individuals to find a match in the database. It is claimed that the system has yet to produce any false positives; processing 2.7 billion comparisons per day, the system has prevented the re-entry of 9,500 persons (Kabatoff & Daugman, 2008).

2.3.3.4 US VISIT program

In response to the 9/11 terror attacks, the United States government sought to secure the integrity of their immigration system, by apprehending or tracking dangerous individuals as they entered the country. The system was officially deployed in 2004 at over 150 different sites (EPIC, 2007). The system has been plagued with problems since its inception.

One of the biggest concerns was the system's dependence on fingerprints, and the amount of function creep to which the fingerprints are susceptible. Originally intended for the verification of visas, the system did not make use of any biometric information, and kept inter-agency interaction to minimal. After the terror attacks, biometrics were introduced, and the programme eventually expanded to cover all individuals travelling to the US (Privacy International, 2004). Additionally, the information collected by the US VISIT program is now cross checked against various other systems (criminal databases, etc.) for which it was never intended.

During its operation in 2005, 150 complaints of errors were filed, including aircrew members who had already successfully passed background checks (EPIC, 2007). As of 2006, the media has reported that the US-Visit scheme has only caught one terror related suspect since its inception (Morgan, 2006).

Furthermore, governments and members of the general public consider the system to be discriminatory. The Brazilian government has retaliated by setting up systems that would require the fingerprinting of all US visitors to Brazil (BBC, 2003). Local US businesses have also expressed worry about the effects of current extensions or problems of the US VISIT program (San Antonio Express, 2008). A recent report claims that the US saw an 11% drop in visitors since 2000 (Collis, 2008); the security procedures in place are believed to be one of the contributing factors: individuals do not feel welcomed as they are treated like suspects on arrival.

2.3.4 Proactive Criminal Investigation

Identification for the purposes of law enforcement has typically been driven by the need for greater accuracy for individual identification. However, new techniques like that of DNA typing *"is that plus much more"* (Cole, 2001), adding capabilities to identify group affiliation and hereditary conditions. The possibility of linking individuals to group affiliation allows authorities to generate more complete portraits of the individuals in question.

Recently, the British government has been considering the possible use of DNA as a tool for identifying nationality (Lettice, 2007). However, this is impossible, given that nationality is not a biological trait but an artificial grouping of individuals into a community (B. Anderson, 1991); it can be assigned and revoked to individuals from a variety of backgrounds, making DNA matching to nationality unfeasible.

Other developments of government and identity assert more proactive approaches in trying to keep track of identity and potential criminals. For example, the British government has been discussing the option of introducing a database of children who exhibit behaviour that might possibly signal criminal behaviour later on in life (Every Child Matters, 2007). National children databases would allow authority figures that come into contact with children to report on their behaviour and conduct. This then allows for the tracking of unwanted behaviour that might eventually lead to serious crime. Unfortunately, systems like these remove the subjective judgements that are important when dealing with vulnerable children and their need for support (see 2.3.4.2).

A strong trend in the development of criminal identity systems is made apparent through a review of past and present systems. Initial concern was the identification of re-offenders. Using forensics, efforts then moved towards accurately identifying criminals the first time through. Now work is being done in predicting who will become criminals. The question of identity thus evolves from the point of establishing it with some other incident in the past (recidivists), to securing the identity of individual to current events (forensics), and now to guessing the identity of individuals in the future (prediction).

Surveillance techniques driven by the bureaucratic drive for rationalisation and prediction materialise here. Additionally, the technology strand of surveillance theory is also relevant (Lyon, 2002). This branch of theory takes the stance that surveillance is a technology-driven need looking for the best mode of operation. In this view, surveillance technology is a self-augmenting and all-embracing quest for perfect knowledge. The technology results in a form of determinism where technology shapes and constructs society, thus allowing it to perform its function.

2.3.4.1 UK DNA database

"DNA is genetic material that determines, in part, individual characteristics that are faithfully transmitted from parent to offspring" (Bieber, 2004). The human genome only varies by about 2 per cent; these variations typically appear in the non-coding regions of DNA sequences, i.e. the sections of genetic material that have no function (Cole, 2001). DNA typing makes use of these variations by analysing DNA for variant lengths and sequences (alleles) at specific sites (loci). These variations can then be compared across samples for identification purposes, and in comparison to fingerprints, DNA provides superior forensic applications (Sankar, 2001).

Established in 1994, the UK currently has the largest DNA database in the world, holding samples retrieved from crime scenes and convicted criminals (Parliamentary Office of Science and Technology, 2006). However since 2004, it has been legal to obtain and store DNA samples from all suspects, even those who have been acquitted of all charges (Wallace, 2006). The situation has resulted in much controversy. The European Court of Human Rights has ruled that the retention of the DNA of un-convicted individuals is unlawful (BBC, 2008c; The European Court of Human Rights, 2008). The current government is proposing to delete hundreds of thousands of profiles from the DNA database, making it illegal for police to retain DNA from un-convicted individuals (BBC, 2011a).

The DNA database has also raised other issues of privacy surrounding the function creep of DNA usage. The Chief Constable in charge of the database regularly receives requests for matching to be performed for paternity cases; even though these are refused, the risk of paternity suits has been cited as a reason why police officers do not want their DNA to be stored on the databases for elimination purposes (Bennetto, 2000).

The authorities have also experimented with new techniques for identification, such as *familial searching* to assist their investigations (Bhattacharya, 2004). For example, familial searching was crucial in solving the 1988 murder of Lynette White in Cardiff (BBC, 2006). The search of the database for a rare gene profile, lead the police to a 14-year-old boy, who was in fact a nephew of the murderer, Jeffery Gafoor; Gafoor received a life sentence in 2003. Another example came in 2004, police managed track down and convict Craig Harman for manslaughter in Surrey; not being on the database himself, police managed to track him down through a relative that was (Bhattacharya, 2004).

Furthermore, just as with dactyloscopy, the infallibility of DNA typing is also in question. Individuals have been sent to prison on the grounds that their DNA matches samples extracted from crime scenes (BBC, 1999; Thompson, Taroni, & Aitken, 2003). In 2007, Mr Easton was accused of a burglary after his DNA produced a match to a crime scene sample in Bolton, Manchester (BBC, 2007). Mr Easton had given a DNA sample 3 years earlier for being involved in a family dispute; the police then found the matched when while they were going through unsolved cases. However, Mr Easton is suffering from Parkinson, and clearly could not have committed the crime. However, a second DNA test to clear his name led to another positive match. This ordeal lasted four months before law enforcement officials were satisfied that Mr Easton is innocent.

DNA evidence was also pivotal in the case of Madeline McCann, who at the age of 3 in 2007, disappeared in Algarve while on holiday from the UK (BBC, 2008b). The local Portuguese police claimed to have found DNA evidence matching Madeline in the car that her parents hired 24 days after her disappearance (Rayner, Gammell, & Britten, 2008; The Independent, 2007). Following this, the McCann's became prime suspects in the 'accidental killing' of Madeline, and were vilified by both the media and the general public in the UK. However, forensic experts in the UK who conducted their own tests found the DNA evidence to be of little value, and greatly exaggerated. By the time the Portuguese police closed investigations, the McCanns were no longer suspects; Madeline remains missing to this day.

2.3.4.2 Contact Point

The death of six-year-old Victoria Climbie due to child abuse was a source of great controversy in 2000 (Laming, 2003). The Every Child Matters (ECM) programme was launched in response to the perceived inadequacies of child protection services; ECM is a programme that called for the sharing of children's personal information, across various services, aiming to ensure the well-being of children.

Contactpoint, a database holding information on all children in the UK, is thus a key element in the ECM programme (Every Child Matters, 2007); it holds information on a child's name, address, and gender, as well as a listing of all the carers and services with which the child comes into contact. However, critics claimed that it would not work as it wasn't the lack of information surrounding child abuse cases, but the way the carers interpreted the information. This view was supported by the death of 17-month-old *Baby P*; carers across various services, who came into contact with *Baby P,* were aware of each other and had all the information, but still failed to interpret the trail of abuse that eventually led to the child's death (Henry, 2008). It is argued that Contactpoint only increases bureaucratic burdens on carers, serving only to hamper subjective process of assessing abuse cases (Munro, 2008).

Other concerns of the Contactpoint database stem from its potential use as a tool for pre-emptive criminal identification. Debates to introduce a similar system has taken place even before the Victoria Climbe case, except its aim was to identify children at risk of offending; *"It actually represents a broadening of child protection services from protection to that of welfare and from there primary and secondary crime prevention"* (Anderson et al., 2006). This is in line with the idea expressed in the *"tough on the causes of crime"* slogan that the UK Home secretary subscribed to in 1993. This potential use of Contactpoint raised much opposition, who cited issues of *e-discrimination* (Anderson et al., 2006), and *self-fulfilling prophecies* (Murray, 2008). Arguments centred on the fact that irresponsible behaviour is not a good indicator of future criminality. Contactpoint could potentially result in the digital branding of children; just as physically branded criminals faced stigmatisation, behaviour towards children that have been digitally branded may be altered, thus pushing them in the direction of unlawfulness. Contactpoint was shut down on the 6th of August 2010.

2.4 An Analysis of Problems

The past and current global situation is filled with diverse examples and experiences of N-IDMSs. While differing contexts and conditions means that no two systems will exactly mirror each other (London School of Economics, 2005), one can still identify common insights that requires further investigation.

2.4.1 Consequences of IDMS Implementation and Use

One of the lessons that can be learned from the review is that the implementation and use of N-IDMSs has a very real impact on individuals' lives and opportunities, as well as influencing their treatment by society.

For example, the N-IDMS deployed in Nazi Germany had a chilling effect on the Jewish population. Intended to make individuals more visible, the N-IDMS constantly exposed individuals' to the rest of society, thus paralysing the individuals while turning the rest of the population against them. A similar effect is seen with the French anthropometric passes for gypsies, where the N-IDMS was designed so as to capture and display their *otherness*; coupled with strict rules, many individuals were forced to change their way of life, abandoning their culture altogether.

The US VISIT programme provides an example where the choice of low quality data sources has resulted in a negative outcome for individuals. Producing a lot of false matches, many innocent individuals were thus wrongly identified as dangerous criminals or terrorists, resulting in a restriction of their movement. Conversely, schemes such as the Schengen agreement, helped to provide more opportunities to individuals, by reducing information checks at borders.

2.4.2 Acceptance of IDMS

Another insight gained from the review is the importance in considering individuals' acceptance of new N-IDMS. Without support from the very individuals who are to enrol, it is unlikely that the system will fulfil its purpose.

The Poor Laws provides a prime example where individuals' perceptions were not taken into account. Forced to constantly display badges that marked them as being poor, individuals felt shame when enrolled into the system. In addition, individuals were aware that their children could be taken away, if they enrolled. As a result individuals refused to enrol, resulting in the failure of the system, and thus created bigger problems where individuals turned to crime instead.

In the Russian Internal Passport system, individuals were clearly not content on serving a particular 'master', in a particular area. Thus the IDMS tying them to a particular location resulted in a mixed success, as a large number of manhunts were launched to track individuals who were not happy with the system.

Furthermore, culture may also play a part in influencing individuals' acceptance of identity systems. In 2003, a Canadian based committee, tasked with investigating the various approaches to N-IDMS, noted that cultural differences between countries affected the citizen-government relationship, and hence had an effect on the acceptance of systems (Fontana, 2003). For example, the British population have always been critical towards the introduction of identity cards, especially when compared to other countries in Europe who have had a long history of N-IDMSs.

The use of the Bertillon system in France and Argentina further highlights the differing reactions caused by differing cultures and perceptions. In France and most other countries where Bertillonage was adopted, there was no public opposition to the collection and use of anthropometric measurements. Argentineans, on the other hand, resisted these measures, viewing them as an insult to their honour. As a result, judges regularly ordered the destruction of the anthropometric records, rendering the system ineffective.

2.4.3 Purpose of the IDMS

Lastly, it must be recognised that the organisation plays a central role in the implementation of the system. It is the organisation, its purpose, and requirements that will drive the implementation and use of the system.

Nevertheless, most organisations today tend to see identity as an all-in-one solution to a myriad of problems. Yet, it is not clear how organisations devise their identity requirements and policies. This has resulted in the implementation of ineffective and potentially dangerous IDMSs.

For example, the law authorities and the general public have come to lean very heavily on forensic matches to crime scenes as proof of guilt, even in the presence of contradictory evidence. Additionally, the current intention to predict the identity of future criminals further emphasises the reliance placed upon identification systems. More evidence of this identity dependence comes from some of the arguments to support the implementation of N-IDMSs. Common justifications include the reduction of crime, illegal immigration, benefit fraud, identity theft and terrorism. Yet, there appears to be little discussion on how identity will integrate into current systems or procedures ensuring the realisation of the benefits claimed.

Another example comes from the US Visit programme. The system is not only ineffective, but has negatively impacted innocent individuals. This is largely down to the failure in not considering the organisations identity requirements in its context of implementation, thus resulting in the poor choice of fingerprints. Compare this to the successful use of iris recognition in the UAE border control scheme.

Therefore, it is critical that organisations consider their identity requirements when implementing IDMS. Who is the system supposed to identify? What are the accuracy requirements? Who will have make use of it? These are all basic questions that help to ensure the IDMS will fulfil its purpose.

2.5 Chapter Summary

A review of past developments sheds light on the effect that the transformation and evolution of administrative practices has on the identity requirements placed upon society. The migration from oral memory to written records emphasised the need for written forms of identification, just as the current shift towards the digital medium brings with it the necessity of digital identity that will allow users to interact in the virtual world.

History reveals the importance placed on the efficiency and accuracy of identification techniques. The primitive use of symbols, insignias and passes were readily doctored, and eventually gave way to verbal portraits to secure identity. Anthropometry eventually gave way to the more accurate method of dactyloscopy, establishing objective forms of identity based on the stable aspects of a person's body. Modern biometric solutions such as DNA seek to further reduce the uncertainty of identity. Currently, identification techniques seek to predict future identity of individuals; what better way to efficiently identify an individual than to predict who a person shall become?

The emergence of nation states after World War II also represented a powerful force in steering the path of identity systems, allowing governments to embrace their people. The governments' social responsibilities, coupled with issues of migration and crime, was a large catalyst in the implementation of identity schemes. Current developments resonate with government efforts to embrace their people. For example, electronic identification systems allow geographically distant citizens to access services and information regardless of their location.

Fear has also played a major role in the history of identity. Examples can be obtained from the discriminatory systems developed because of the perceived otherness of certain groups, such as the gypsies in France. The insecurity produced during periods of war also gave rise to the need for identity systems; the establishment of National ID Systems in the Britain during World War I and II illustrates this point perfectly. Additionally, the rule of totalitarian regimes also resulted in strict controls of identity. Nationality, group segregation, and a need to control resources drive such regimes towards identity systems so as to better control the population.

Throughout the review, it was evident that the human component was critical in determining the success or failure of an IDMS. From the feelings of shame in the Poor Laws, to an insult of honour in the Bertillon system; from the prussianizing perceptions of the of the British identity cards to the confusion around digital signatures; from the privacy concerns of DNA identification to the self-fulfilling prophecies of predictive criminal identification, it is this human component that IDMS must account for.

In reviewing the N-IDMSs, research into identity systems need to account for the real impact that a system has on individuals that are enrolled. Furthermore, research also needs to develop an understanding of individual acceptance towards N-IDMS, of which culture may also have an influence.

Last but not least, the review has also highlighted the importance of organisations purpose and requirements in defining the overall structure and implementation of an IDMS. It is therefore crucial that research seeks to understand what organisations need, and how a balance can be struck between the organisation and the individual.

Chapter 3: Literature Review

This chapter reviews the published literature within the identity field, identifying gaps that this thesis will address.

Beginning with the concept of identity itself, the review in Section 3.1 uncovers that current research is limited to functional perspectives, where individuals are treated as functional objects. This approach ignores the concept of identity as strategic information to inform organisational processes (for example the UK government's intention to use the N-IDMS to combat terrorism by using an audit trail to investigate suspected terrorists; Section 7.2.2.2, or the intention to use the Contactpoint child database to identify future criminals; Section 2.3.4.2). As a result, most 'human-centred' identity solutions tend to focus on usability issues and the reduction of barriers to getting individuals to share information, instead on the broader impact of identity.

The consequence of the functional view of identity becomes evident in Section 3.2, where the review of the privacy literature reveals that research has focused on *information privacy*. The emphasis is on a *confidentiality* paradigm, which does not explore the consequences of identity information collection, storage, and use (for example the *paralysing* effects of the Nazi's N-IDMS [Section 2.2.2.1] or the lack of perceived benefits in the Austrian Citizen Card [Section 2.3.1.2]; these effects of system design on the lived experience are studied and detailed in Section 5.2). Recently researchers have called for a broader approach, focusing on the protection of identity, instead of the protection of information as a static concept (Section 3.2.4.3).

Moving on to the concept of trust, the review in Section 3.3 finds that past research does not consider the impact of identity on individuals' trusting behaviour; specifically, it does not account for how system design can influence *perceived risk*, and thus affect individuals' intentions to trust and adopt IDMSs.

Finally, this chapter also reviews the concept of culture, and how it can affect individuals' trusting intentions (Section 3.4). Understanding the impact of culture can be useful because it helps to explain the differences between the privacy and trust reactions of populations from different countries (for example, *individualistic* cultures are highly critical and vocal of systems that restrict their freedoms; this is explored in the study outline in Section 6.5.2).

3.1 Identity

Being part of everyday language, many feel than the term identity is widely understood, and see no need to define it. This is one of the problems that researchers and implementers face; a proper definition of identity is required in order to fully study the phenomenon of interest, as well as to increase understanding among the research community. This chapter will define identity as it is used in this thesis; in order to do so, several different definitions that have been put forward are reviewed and their respective shortcomings described (Section 3.1.1).

This chapter will also explore the concept of an IDMS, and the various configurations that these systems can take (Section 3.1.2). The chapter then looks at the current approaches that focus on creating a user-centric approach to IDMS (Section 3.1.3). A review of the literature shows that research in the area focuses on identity as a means for access control, only seeing it as a mechanism to allow individuals to access restricted resources. Current efforts do not explore identity in terms of strategic information that is being used by an organisation, how it relates to the individuals that are seen as static objects that are disconnected from the real world.

3.1.1 Defining Identity

> *"The worst thing one can do with words, wrote George Orwell'…'is to surrender to them'…'let the meaning choose the word, and not the other way about.' Identity, we argue, tends to mean too much (when understood in a strong sense), too little (when understood in a weak sense), or nothing at all (because of its sheer ambiguity)."* (Brubaker & Cooper, 2000)

Pfitzmann & Hansen (2010) define identity as an individual's bounded concept that represents a perception of life, social interaction and continuity. This explains the lack of clarity regarding identity, as this bounded concept varies across individuals. Furthermore, identity today can refer to a number of nouns and concepts; it can be interpreted as a set of personality traits, or just as commonly to refer to a hashed password (Camp, 2004a). With the growing importance of identity and IDMS, there is a growing need to accurately define identity, typically in terms of information collected and stored about an individual.

3.1.1.1 Identity and its building blocks

A proper definition of identity first requires an understanding of its basic building blocks. There are two core constructs that make up an identity in the computing field, and are defined by (Camp, 2004b), as follows:

1. **Attribute.** A characteristic associated with an entity. Examples include long-lived characteristics such as height and date of birth, as well as temporary attributes such as address and employer.
2. **Identifier.** An identifier identifies an identity within a specific context. An entity can have many identifiers; for example, a car has a license plate but also a permanent serial number. *"Each identifier is meaningful only in a specific context, or namespace, and can reasonably be thought of as having a <thing identified, identifier> pair"* (Camp, 2004b).

An understanding of these two components allows for the definition of identity; continuing from above, (Camp, 2004a) defines identity as a *"set of permanent or long-lived temporal attributes associated with an entity"*. This definition diverges from other definitions in the field, as it fails to account for the uniqueness of identity within a system. Cameron (2005) also does not capture this aspect when defining identity as *"a set of claims made by one digital subject about it-self or another digital subject"*. Furthermore, this definition confuses the concept of identity with the entirely separate process of identification; i.e. the definition alludes to the process of presenting an identity to another entity, rather than defining what exactly the claims might be.

An alternative definition of identity comes from White (2008), who states that identity is *"a set of characteristics, or identifiers, of an entity that uniquely identifies that entity within a specific context or system."* Similarly, in developing an ontology of identity-related terms, Pfitzmann & Hansen (2010) define identity as *"any subset of attributes of an individual person which sufficiently identifies this individual person within any set of persons."* While these definitions capture the essence of uniqueness, the definitions are aligned more with the concept of an identifier, which is but one part of an identity; it fails to fully recognise the importance of the attributes and information attached to an identity.

3.1.1.2 Attributes, partial identity and context

Identity does not exist in a vacuum; it is established on the basis of interactions with others, and its content is defined by the role that an individual assumes in each interaction. Each role consists of a set of attributes relevant to the particular context, and this subset of relevant attributes, in relation to the particular role, is termed a *partial identity* (A. Pfitzmann & Hansen, 2010). An IDMS should therefore aim to instantiate individuals within the system, by capturing the attributes that make up the partial identity, allowing individuals' to carry out the tasks in relation to their role.

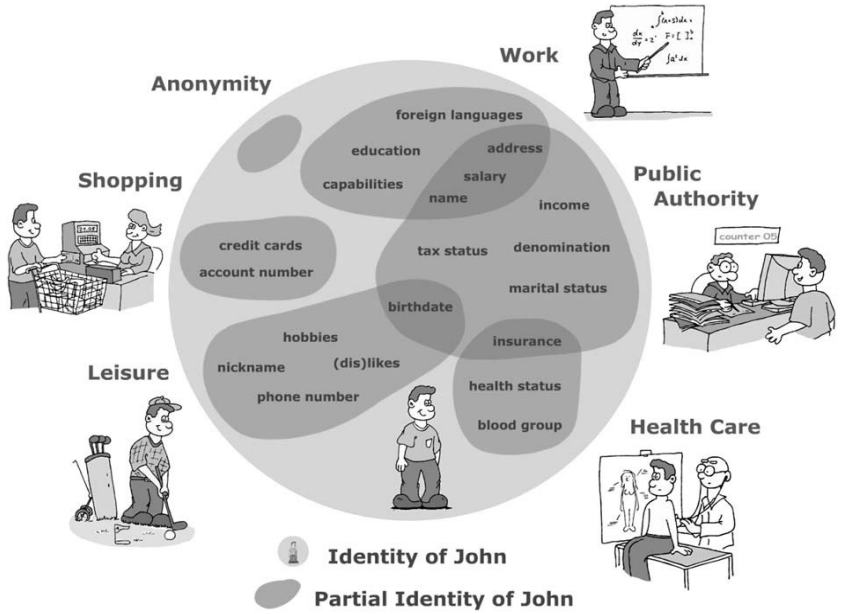


Figure 3 Partial Identity (Pfitzmann, Hansen, Liesebach, Pfitzmann, & Steinbrecher, 2006)

However, in order to fully research identity and its impacts, we must consider richer forms of identity that go beyond the standard definitions. The *data shadow* refers to the collection and storage of various types of information about an individual, stretching beyond the traditional definition of identity as attributes (Garfinkel, 2001). It is the data trail that an individual leaves behind with every transaction (every cash withdrawal, every credit card payment, etc.); highly dynamic new information is constantly produced, and is attached to an individual's identity within the system. Brought together, this information forms a *digital dossier* (Garfinkel, 2001) of a subject that can then be used by the organisation; individuals' interaction with organisations will probably be mediated by the *data shadow*, and not solely on the basis of the individual's inherent attributes.

It is therefore important that a definition of identity express the uniqueness of an identity, while at the same time capturing the depth and reach of the identity. For the purposes of this research, identity is defined as the set of information and attributes about an individual that is collected and stored within a particular context; linked to an identifier(s) that sufficiently identifies the individual within as set of individuals.

3.1.2 Identity Management Systems (IDMS)

The literature simply defines an IDMS as a system that enables the administration and use of identities, and their attributes. Within a government context, White (2008) states that identity management is the administration of identity, *"so as to provide secure and controlled access to the resources that an entity is entitled to use"*. Pfitzmann & Hansen (2010) describe identity management as *"the administration of identity attributes including the development and choice of the partial identity… to be (re-)used in a specific context or role"*.

These definitions, as with the typical definitions of identity, are insufficient as they confine identity management to the realms of access controls, disregarding other potential uses, such as the use of identity to power recommendation systems. These definitions of identity management have probably contributed to the traditional focus on *Type 1 IDMS* as described by Bauer, Meints, & Hansen (2005):

1. **Type 1 IDMS** used for account management, implementing authentication, authorisation, and accounting.
2. **Type 2 IDMS** used for profiling of user data by an organisation, e.g. detailed log files or data warehouses that support analysis of customer behaviour.
3. **Type 3 IDMS** used for user-controlled context-dependent role and pseudonym management.

While the initial development of IDMSs may have largely served to act as an access control mechanism, reflecting Type 1 IDMS, hybrid configurations are now becoming more common, i.e. systems that fit into two or three types of IDMS configurations, such as social networking and recommender systems (Mentis & Zwingelbery, 2009). It is therefore imperative that research accounts for the current trends in the field.

As such, an IDMS can be defined as a mechanism that allows for the administration of information and attributes of an identity; and its use by individuals to gain access to resources, as well as its strategic use by organisations to inform business processes and decision-making.

3.1.2.1 The identity lifecycle and models of IDMS

Identities instantiated within an IDMS typically go through a set of phases. According to Hansen, Pfitzmann, & Steinbrecher (2008), these phases are establishment, evolution, and termination of identity. Similarly, Windley (2005) states that an identity starts out by being provisioned, after which it is propagated though the system, where it gets used, maintained, and finally de-provisioned. In general, the IDMS literature typically expands upon the lifecycle relation to traditional Type 1 IDMS. The phases of identity described below are an amalgamation of commonly established processes encountered in the literature:

1. **Enrolment.** The creation of new identities within the IDMS. It involves the identification of relevant individuals, the capturing of their attributes, and the instantiation of their identity. Authentication credentials are generated and provided to each individual allowing them to use it.
2. **Provisioning.** The back-end management of identity, where identities within the system are given permission to access certain resources; i.e. access policies.
3. **Identification.** The process whereby an individual presents his/her identifier and credentials to the system; the individual presents a claim that he/she owns the identity linked to the provided identifier.
4. **Authentication.** In this phase the IDMS takes the identifier and credential provided in the previous phase, and checks that it is valid. Failure to produce a valid identifier-credential pair will prevent an individual from accessing the system.
5. **Authorisation.** If authentication was successful, the system then retrieves the access permissions that were attached to the identity during provisioning. The individual is then provided access to the resources to which he/she is allowed to access.
6. **Maintenance, deletion, and auditing.** Typically there is also a mechanism by which identities can be edited, where identity is updated to reflect new information, and audited for security purposes. Identities can also be deleted from the system, where the identity, and all related information is purged from the system. However, in modern systems, identities may not be deleted or suspended.

An inspection of the stages in the identity lifecycle quickly reveals the emphasis placed upon the use of identity as an authentication mechanism; i.e. the lifecycle describes a Type 1 IDMS implementation. There is no recognition of the back-end use of identity information, by an organization, to inform its practices or functions. This aspect of identity usage, a core function of Type 2 systems, has been side-lined in the literature (although investigated to a point from a social science aspect under the umbrella of surveillance studies; see Lyon (2002) for an example).

Thus, following the focus of high-level identity descriptions on Type 1 configurations, current identity literature has focused on Type 1 related issues of functionality and usability. Similarly, IDMS architectures have been developed around the Type 1 viewpoint, where identity is only seen as a means of accessing resources, while failing to account for identity as the strategic resource that is being accessed by the organisation in the back-end (White, 2008).

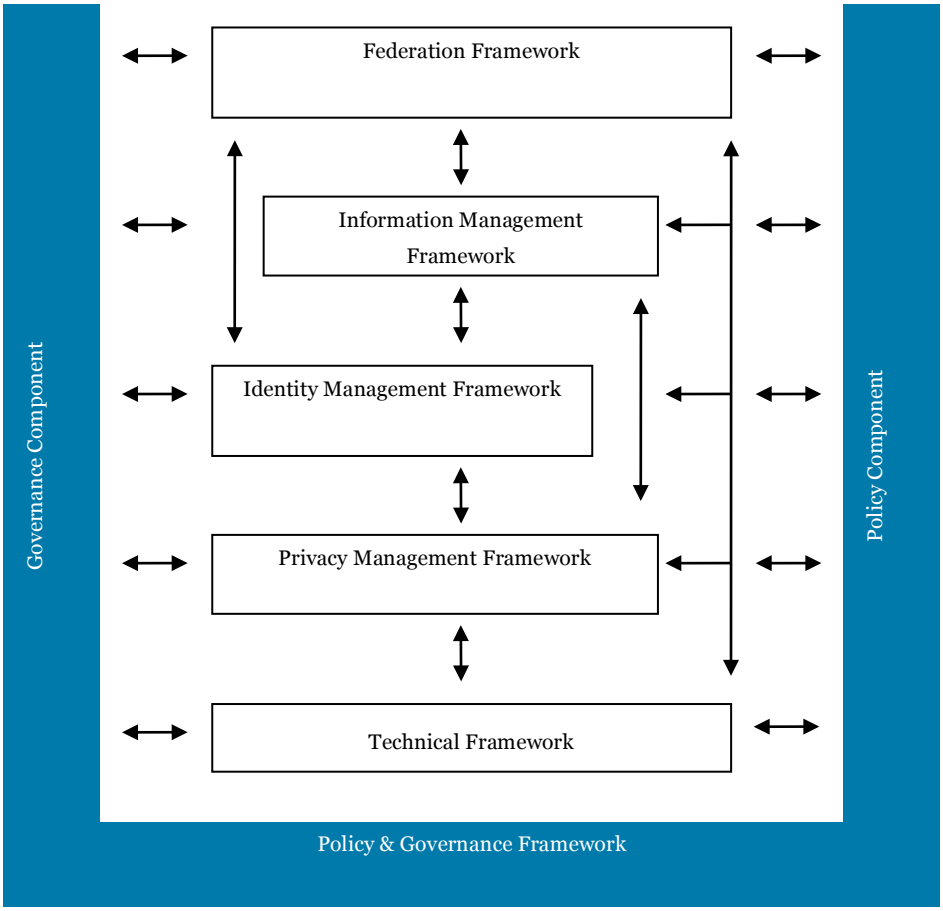


Figure 4 Identity Management architecture (White, 2008)

3.1.3 User-centred Identity

Following the typical description of the identity lifecycle, common research into *user-centric* identity systems also falls within the realm of type 1 IDMS configurations, where identity is actively used by an individual to access privileged resources. In the era of networks and distributed services, research into user-centric identity manifests itself in the form of federated schemes, which aim to make it easier for individuals to use their identity.

Traditionally, services exist within silos; each organisation (i.e. service provider) implemented a standalone IDMS to work with their own systems. With the increased level of services being provided online, individuals are required to memorise a large number of passwords, making such systems unmanageable and causing identity overload and password fatigue (Jøsang, Zomai, & Suriadi, 2007).

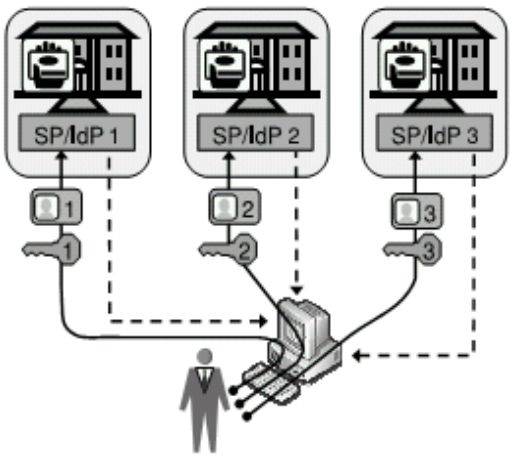


Figure 5 Silo model of IDMS (Jøsang, Zomai, et al., 2007)

Aiming to reduce these barriers to adoption, federated identity schemes have been proposed as a solution to create user-centric identity management. Federated identity is a *"set of agreements, standards, and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain"* (Jøsang & Pope, 2005). This allows individuals to enrol with a single organisation (i.e. identity provider), and use the resulting identity credentials to login to other service providers that are separate from the identity provider. OpenID is an example of a federated identity scheme, and is being used and supported by Google, Yahoo, and Facebook among others.

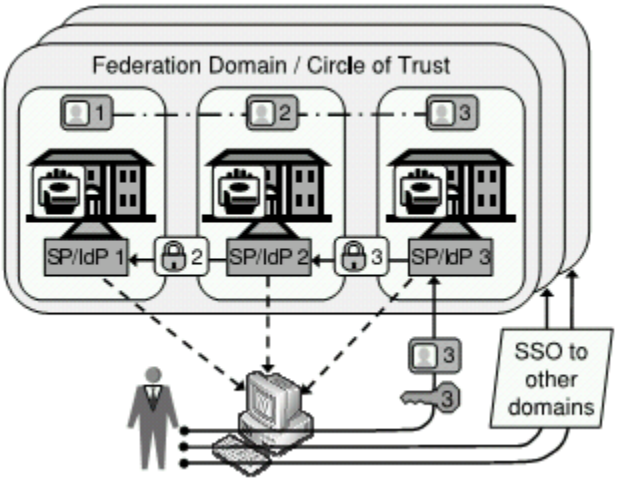


Figure 6 Federated model of IDMS (Jøsang, Zomai, et al., 2007)

Similar efforts in the area of user-centric identity are the development of an *identity metasystem* (e.g. Info-Cards, Higgins, etc.). In recognising that the identity on the internet is a *"patchwork of identity one-offs",* Cameron (2005) suggests the creation of an identity layer that abstracts away from the internal complexities of identity systems, allowing various standards and technologies to work from similar user-interfaces. In line with this, he developed a set of seven laws that would guide the development of an identity system with the objective of creating a system that is widely accepted:

1. **User control and consent**
2. **Minimal disclosure for a constrained use**
3. **Justifiable parties**
4. **Directed identity**
5. **Pluralism of operators and technologies**
6. **Human integration**
7. **Consistent experience across contexts**

3.1.4 Limitations of Current Identity Research

Current approaches to identity do not recognise it as strategic information that alters individuals' interaction with organisations and the larger identity ecosystem.

This is largely driven by the traditional role of identity within Type 1 IDMS configurations, where identity is used as a security mechanism used to access resources. As a result, user-centric research (Section 3.1.3) on identity is generally focused on ease of use, to encourage individuals to enrol in the system, without examining the strategic usage of identity and its effect on the individual (see for example federated identity that attempts to eliminate barriers to sign up and information sharing).

Human-centred IDMS research should not only consider ease of use, but also take into account the relationship between identity and the individual, break away from the Type 1 view of IDMSs, and focus on the broader implications and uses of identity. Identity is not just a static component, its use has impacts on the individuals and the world around them; the influence of this concept on the approach taken in this thesis is further clarified in the review of the privacy literature in the next section (Section 3.2).

3.2 Privacy

> *"A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy… Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech" (Australian Privacy Charter)*

Traditional approaches to privacy do not acknowledge the wider implications of identity on everyday lives. As this review will reveal, privacy research sees identity information as a static component, resulting in approaches that focus on confidentiality rather than protection of identity and the individual.

Privacy can be defined in relation to the *physical, psychological, interactional and informational* realms (Section 3.2.1). The nature of computers and their use in the collection of personal information has placed an importance on the *informational dimension of privacy* in computing literature. Studies seeking to capture individual's *informational privacy* concern focus on the *collection of information, the errors that may occur during collection, its unauthorised use, as well as improper access to subject information*. However, other research has shown that individuals tend to view privacy concerns in terms of the potential outcomes (Section 3.2.2).

With the focus on *information privacy*, approaches addressing privacy concerns have led to the development of *Privacy Enhancing Technologies* (Section 3.2.4) that focus on *data minimisation* and *anonymity*, which do not fully address the impact of identity on the individual (Section 3.2.4.1); i.e. the *lived experience*. Furthermore, emphasis on *information privacy* has also influenced the development of laws and regulations to focus on the collection and storage of information, as opposed to the focus on identity itself (Section 3.2.4.2). Recent debates have called for a rethink of the legal infrastructure, seeking to establish the *right to identity* (Section 3.2.4.2).

Further research into privacy and IDMS should therefore focus on the consequences of identity, and how it can affect the individual. Research should look at the *lived experience of identity* (Section 3.2.5).

3.2.1 What is Privacy?

Anyone involved within a society has to balance the notion of privacy. Some have defined privacy as having *"the right to be left alone"* (Warren & Brandeis, 1890), while others question the simplicity of this definition. In part, the difficulty in agreeing on a single definition of privacy stems from its multi-dimensional nature. For example, Burgoon (1982) introduces privacy dimensions relating to the *physical, social, interactional, and informational.* This is somewhat reflected by Davie's (1999) concept of *data, communications, bodily and territorial privacy*; while DeCew (1997) identified concerns with regards to *informational, accessibility and expressive privacy*.

Whatever the case, the number of privacy debates is increasing. Not long ago, one would be able to stand in an open field to guarantee a private conversation; however, this is no longer possible with the array of devices available. Technology has an inherent ability to erode the walls of privacy that we build around ourselves. The mechanisms of today allow for easier collection and storage of data; the decline in storage costs permits for larger collections of data that can then be stored for longer periods of time, while ubiquitous computing introduces the ability for the recording of timely and accurate location data (Anderson & Dourish, 2005; Bellotti & Sellen, 1993; Price, Adam, & Nuseibeh, 2005; Smith, LaMarca, Consolvo, & Dourish, 2004). Meanwhile, network infrastructures allow information to be traded easily among organisations, enabling new deductions to be made, and hence creating more privacy invading situations (Palen & Dourish, 2003).

Recently, developers have begun to take privacy design seriously; many researchers and developers believed that individuals and society would adapt their privacy expectations and behaviours to fit in with new technology. Adams & Sasse (2001) paralleled this early view of privacy with similar notions in early *human computer interaction (HCI)* debates; it was initially argued that users would learn and familiarize themselves with highly unintuitive interfaces. This of course has been proven false, and HCI is now considered an integral component in the design of successful applications.

Similarly, researchers and system designers are now taking the issue of privacy seriously, working to eliminate or reduce the risk of privacy invasions when developing new systems (Iachello & Hong, 2007). Due to the technical nature of Computer Science, and its focus on the collection and storage of personal information, privacy research in the field is largely focused on the issue of *information privacy*.

3.2.2 Individual Privacy Concerns and Behaviour

The concept of privacy is invariably tied to the individual; it is his/her privacy that is being invaded. However, most research in the area has focused on protecting data without a proper understanding on what exactly individuals deem as being private (Adams & Sasse, 2001; Paine, Reips, Stieger, Joinson, & Buchanan, 2007; Palen & Dourish, 2003). Without a proper understanding of individuals' privacy views, how can systems be designed to enforce them? Unfortunately, therein lies the problem; privacy boundaries are dynamic, and vary between individuals, such that it becomes an ambiguous concept that escapes proper definition (Anderson & Dourish, 2005; Bellotti & Sellen, 1993; Smith, 1993).

Investigating privacy concerns towards the collection of personal information by organisations, (Smith et al., 1996) developed a set of categories that capture an individual's informational privacy concerns. Developed on rich theoretical material, it has a large base of empirical results that verify the validity of the measure. The categories as defined by (Smith et al., 1996) are:

1. **Collection.** The concern over the excessive collection and storage of personal information.
2. **Unauthorised use.** The concern over the use of personal information for other purposes.
3. **Improper access.** The concern over the unauthorised access and use of personal information.
4. **Errors.** Concerns over the occurrence of errors, deliberate or accidental, in the personal information.

However, recent studies into privacy illustrate that individuals more readily associate privacy concerns with the potential negative outcomes of a breach. Paine et al. (2007) found that the privacy concerns of Internet users seem to focus on crime, and not privacy problems; individuals raised issues regarding viruses, spam, spyware and hackers among other things. Therefore, individuals may see the privacy issue as a wider concept than do those in academia, with its narrow focus on information privacy.

3.2.3 Identity and Informational Privacy

In line with the research in the general computing field, common approaches to the privacy problems, presented by IDMSs, are tackled from the information privacy dimension. In the computing field, this has led to the development of *Privacy Enhancing Technologies (PETs)* that focus on the *confidentiality* of personal information. Similarly influenced by *informational privacy*, laws and regulations that aim to address privacy concerns raised by IDMSs focus on the concepts *data protection* and *data minimisation*.

3.2.4 Identity and Privacy Enhancing Technologies

While the increasing use of technology has been the catalyst for the current privacy debates, a lot of work is being done to use technology to enable privacy. In line with the understanding of information privacy, these PETs seek to ensure privacy by minimising the collection and processing of personal information. As a result, the dominant paradigm in the development of PETs has been that of *"privacy as confidentiality"* (Gürses, 2010).

The cornerstone of this confidentiality perspective in the IDMS field is the concept of *anonymity*. At a simple level, anonymity can be defined as the un-identifiably of a subject among a set of subjects. Pfitzmann & Hansen (2008) further describe anonymity in terms of *unlinkability*; unlinkability refers to the inability of an attacker to sufficiently establish a relationship between two items of interests (e.g. an individual and an action); individual anonymity with respect to a particular attribute can therefore be expressed as the *"unlinkability of an individual to the particular attribute"*. Popular mechanisms by which PETs achieve this unlinkability are the use of pseudonyms to hide an individual's true identity, and encryption techniques that transform data into unreadable form (Senicar, Jerman-Blazic, & Klobucar, 2003).

3.2.4.1 Beyond confidentiality

Reviewing PETs in their early stages, Burkert (1997) identified as one of its limitations, the *"capability to identify persons behind anonymous information"*. By pooling together and matching information from various anonymised sources, an individual can be re-identified with sufficient accuracy so as to take discriminatory measures (Burkert, 1997). Gürses (2010) further expands on this idea, stating that *"anonymously collected data does not protect against surveillance systems, and the reflexes of their controllers to manage and sort populations"*.

PETs can create a false sense of autonomy and control, since information collectors are still able to manipulate behaviour using anonymised information. While Gürses (2010) sees PETs as being useful, she suggests newer approaches that focus on the control of information, how it is used, as well as creating more engagement between the individual and the flow of his/her information. Hildebrandt (2008) suggests something similar in the form of *Transparency Enhancing Tools (TET)* that *"renders accessible and assessable the profiles that may affect their lives"*.

3.2.4.2 Privacy laws and data protection

Development of laws and regulations designed to limit the privacy-invading aspects of IDMSs date back to the 1960s, with respect to proposed plans for centralised database systems. The response was the codification of the first set of data protection laws (Mayer-Schönberger, 1997). Today the European Union enforces a set of *Data Protection Directives*, while the United States has opted for a sectored approach, i.e. relegating privacy policy enforcement to professional bodies.

In a 1998 report regarding the collection and storage of personal data, the United States Federal Trade Commission published a set of recommendations that aim to provide individuals with adequate privacy protections. Codified under the *Fair Information Practice Principles*, the recommendations consist of five core principles (Federal Trade Commission, 1998):

1. **Notice.** *Individuals should be given notice of an entity's information practices before any personal information is collected from them.*
2. **Choice.** *Individuals should be provided options as to how any personal information collected from them may be used.*

3. **Access.** *Individuals should be able to access data about him/her-self and to contest that data's accuracy and completeness.*
4. **Integrity.** *Collectors must take steps to ensure data is accurate and secure.*
5. **Enforcement.** *A mechanism to enforce these principles; self-regulation, private remedies, and regulatory schemes need to be put in place.*

Similarly, the European Union has published the *Data Protection Directive* that aims to protect privacy by focusing on the processing of personal data. The directive ensures that personal information of European citizens will have similar protections across the union. Each country is required to bring their national legislation in line with the directive; the United Kingdom *Data Protection Act* is an example of the implementation, and consists of eight key principles (House of Lords, 1998):

1. *Personal data shall be processed fairly and lawful.*
2. *Personal data shall be obtained only for one or more specified and lawful purposes.*
3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
4. *Personal data shall be accurate and, where necessary, kept up to date.*
5. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
6. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
7. *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
8. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

3.2.4.3 From protecting privacy to protecting identity

Recent debates around these identity and privacy laws are calling for a rethink of the legal infrastructure (Hildebrandt, 2008); a shift for the right of privacy, toward the recognition of a *"right to identity"* (De Hert, 2007). It is argued that *"identity related issues cannot be dealt with from a privacy-perspective"* (Gutwirth, 2009); providing an example, De Hert (2007) elaborates further; *"when homosexuals seek anonymous contacts with others fearing stigmatisation and professional harm, the issue is certainly identity-related, but what kind of issue is it from a legal point of view? A privacy issue? A liberty issue? Or a freedom of movement issue?"*

Lusoli, Maghiros, & Bacigalupo (2009) also call for a new regulatory framework, arguing for the *"need to move beyond discussions about privacy, and move into a full fledge discussion of identity"*. They propose an *autonomy* regulatory framework, which may be viewed as an *"enactment of decisional privacy, whereby citizens can take decisions for themselves and act on those decisions free from external interference"*.

In a similar vein, Hildebrandt (2008) describes the threats of identity profiling on individuals' abilities to construct their identity, as well as the shortcomings of current regulations to address the problem; *"informational privacy is all too often reduced to a private interest in the hiding of personal data"*, thus ignoring the consequences of the knowledge asymmetry between the individual and the profiler. Profiling can create an *autonomy trap* that seduces an individual to act in a manner that he/she would not have done otherwise, as well as allowing for easier market segmentation, and therefore easier discriminations. Lips et al. (2006) describe the effects of *social sorting* within a government context, where individuals are treated differently on the basis of their identity and trust profiles, thus fundamentally changing the relationship between citizen and state; an unequal and discriminatory form of *layered citizenship* is created. In light of these dangers, Hildebrandt (2008) calls for a rethink of the legal framework to understand how profiles may impact individuals' lives in practical ways.

3.2.5 Limitations of IDMS Privacy Research

Privacy in the general computer science, and hence IDMS field, has largely been tackled from the informational privacy dimension. This has resulted in approaches to mitigating privacy concerns through a confidentiality paradigm, seeking to minimise data collection and prevent information from being linked directly to an individual.

The narrow focus on informational privacy may be linked to the focus on Type 1 IDMS, as introduced in the previous chapter. However, IDMS are no longer just used as an access mechanism, but are now widely used in Type 2 IDMS architectures, where individual profiles are used to aid organisational decisions. It is not just the collection and storage of identity that is of concern, but the actual usage of identity that has an impact on an individual's life.

The current debates on the suitability of current technological and legal procedures to solve issues of identity are largely driven by the focus on the outcomes dictated by identity collection, storage, and usage. Autonomy, and the ability to freely develop one's own identity and to avoid being discriminated against, all call into question the suitability and moral uses of identity information. Similarly, research has shown that individuals tend to think of privacy in terms of the implications rather than the information being collected.

In discussing the collection of personal information, Mayer-Schönberger (2009) writes about the dangers of not *forgetting* stored information; he conjures up an image where individuals are *"shackled by their constantly present past"*. Not being able to act and interact with others only in the present, individuals are denied the ability to develop further.

> *"Digital memories make possible a comprehensive reconstruction of our words and deeds, even if they are long past, they create not just a spatial but a temporal version of Bentham's Panopticon, constraining our willingness to say what we mean, and engage in our society"* (Mayer-Schönberger, 2009).

Therefore, privacy research should reflect the current calls of privacy experts to focus on the consequences of identity collection, storage, and use (Section 3.2.4.3). This is in line with individuals' perception of privacy that focuses on outcomes such as being victims of crime (Section 3.2.2). Research should thus look beyond the traditional information domain, and seek to explore the impacts of identity. How does an IDMS influence the life of an individual? In reference to the act of profiling, Hindlebrandt (2008) states that the main concern lies in the *"the process of constructing profiles and their application to people"*. Thus research needs to focus on the design of design of identity and IDMSs, and its affect the outcomes for individuals. Research should focus on exploring the *lived experience of identity* (Rahaman & Sasse, 2011), which captures the main concern identity on individuals' everyday lives.

3.3 Trust

> *"Scholars tend to mention [trust] in passing, to allude to it as a fundamental ingredient or lubricant, an unavoidable dimension of social interaction, only to move on to deal with less intractable matters" Gambetta (1988).*

Trust is a central component to privacy because it mediates for any privacy concerns that arise; for example, providing sensitive personal information to an organisation, requires individuals trust in the organisation to keep his/her information private, while also not misusing or abusing the personal information. An analysis of the trust literature reveals that little work has been done in relation to IDMS, and even then current research does not account for how the design and perceived risk affect individuals' trusting intentions.

Based on the literature, this chapter explores the concept of trust, elaborating it in terms of *risk* and *uncertainty*. Differences between the development of *initial trust* before interaction, and the transition to on-going trust in continuous interactions are also discussed (section 3.3.1).

Several models of trust have been developed to predict individuals trusting behaviour in the face uncertainty. Early models focused on economic perspectives, where trusting actions are dependent on the benefits gained. Current approaches that predict trusting behaviour in e-commerce and e-government systems take a multidisciplinary approach, guided by an overall behavioural framework (section 3.3.2)

A trust model that predicts adoption of N-IDMS was developed and proposed in the literature (section 3.3.4). However, as with many of the current trust models, the proposed model does not fully capture how the system itself can affect adoption (section 3.3.5).

The chapter concludes that it would be highly beneficial for studies to investigate how a system's design, and thus its perceived implications, can affect trusting intention and adoption. In so doing, a better understanding of the overall situation is gained and practical tools or methods may be developed that allow researchers and practitioners to design more trustworthy systems.

3.3.1 Trust and Risk

Trust is pervasive in our daily interactions. It forms an important part of social interactions; without it, we would be incapable of dealing with the world in its endless degrees of risk and complexities (Cofta, 2007; Riegelsberger et al., 2005), as well as promoting co-operative behaviour, and allowing a person to depend on the actions of unknown others (Mayer, Davis, & Schoorman, 1995). In spite of, or perhaps because of its pervasive nature, *trust* eludes a single definition; for example, Mcknight, Cummings, & Chervany (1998) found 17 different definitions of trust when reviewing the literature.

Trust is typically required in situations when there is something at stake, and hence the potential for negative outcomes (Riegelsberger et al., 2005). Therefore, trust is said to be needed when there is an element of *risk* involved; an individual (*trustor*) needs to take trusting action in the hopes that the other party (*trustee*) will act as intended. However, risk in itself is a rather vague concept with various definitions and interpretations.

Risk is sometimes associated with *uncertainty*, and although both terms tend to be used interchangeably, there are slight differences between the two concepts (Riegelsberger et al., 2005); risk typically implies that the probability of a negative result is known, while uncertainty implies that the probability of the outcome is unknown. According to Giddens (1991), trust is no longer required when the trustor's actions, motivations and abilities are known; a trustee is able accurately to come to a conclusion of the risk involved, and hence take a risky action instead of a trusting one. As such, it would seem that trust is better related to the concept of uncertainty than to that of risk. However, situations of risk can be viewed as those of uncertainty by reducing its complexity, eschewing any probability calculations involved (Luhmann, 1979).

3.3.1.1 *Initial Trust and the Expectation of continuity*

The development of trust can be broken down into two distinct phases (Carter & Bélanger, 2005; Warkentin, Gefen, Pavlou, & Rose, 2002). Firstly, there is the concept of *initial trust*, where a trustor has yet to interact with the trustee; in this phase, a trustor's trusting intentions are largely based on personal dispositions and social norms. A separate distinct phase of trust development is that of *on-going trust*. In these situations, trusting intentions are driven by the experience gained through repeated interactions; on-going trust breeds *familiarity* between trustor and trustee, reducing the trustor's perception of risk involved. Familiarity provides trustors with a framework for future interactions based on previous experience, thus increasing the levels of trust (Riegelsberger et al., 2005).

3.3.2 Effects of Trust and Risk on Adoption

Trust research has gained a lot of momentum in the e-commerce and information science domain; it is also gaining traction in the field of e-government. Typically posited as a factor that influences the *adoption* of new services and technologies, initial trust is seen as a mechanism that shapes a trustor's behaviour when interacting with the new service or technology.

In research, trust is typically explored alongside the concept of risk. *"Scholars have provided different views regarding the relationship between trust and risk, i.e. whether trust is an antecedent of risk, the same as risk, or a by-product of risk"* (Kim, Ferrin, & Rao, 2008); in any case, trust is required in situations of risk, making it difficult to uncouple the two concepts.

Several different trust, risk, and adoption models have been developed. From psychology, we have the *Theory of Reasoned Action*, which focuses on behaviour of individuals. The social sciences look at trust from a societal point of view. *Game Theory* places importance on social control in the development of trust, while economical approaches appear to model trust in terms of perceived risk, as well as the potential benefits and losses. Research soon took on a multi-disciplinary approach, accommodating for relevant elements extracted from the various models in the creation of a more complete and more accurate mechanism to assess trust, risk, and its impact on adoption (McKnight & Chervany, 2001).

3.3.2.1 Theory of Reasoned Action and Behaviour

Many current trust models are rooted on the *Theory of Reasoned Action (TRA)*, and its later counterpart the *Theory of Planned Behaviour (TPB)*. In these models trust is expressed as an intention or willingness to carry out a trusting behaviour.

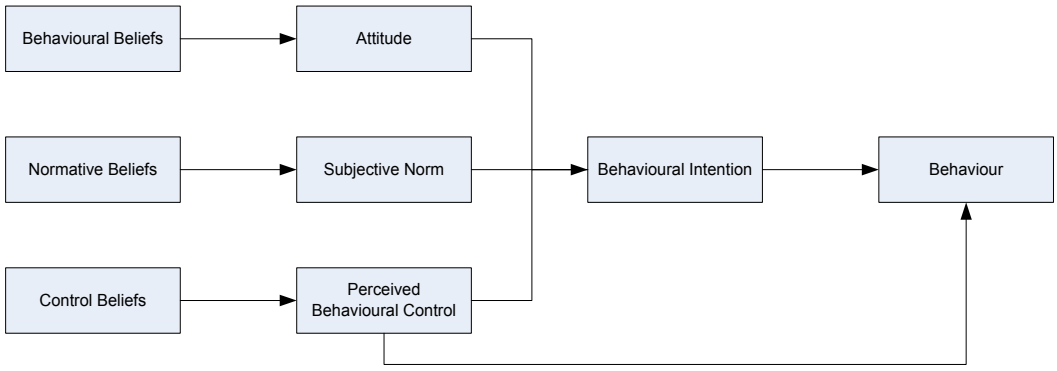


Figure 7 Theory of Planned Behaviour Model

According to the TRA, as described by Fishbein & Ajzen (1975), *intention* to perform a specific *behaviour* is dependent on an individual's *volitional characteristics* that capture the rational and calculative decisions that an individual makes. There are two constructs that make up the volitional component:

1. **Attitude.** A person's favourable or *"unfavourableness towards an action"* (Fishbein & Ajzen, 1975). It is an evaluative bipolar dimension that an individual makes about an object or decision (for example like/dislike, favourable/unfavourable, etc.).
2. **Subjective Norm.** An individual's preconceptions on whether the people closest to him/her think that the action should be carried out.

Later, TPB introduced a non-volitional aspect that can influence behavioural intentions (Ajzen, 1985, 1991):

3. **Perceived Behavioural Control.** An individual's perceptions of the opportunities and constraints on performing the action. Greater perceived behavioural control positively influences intention. Additionally, perceived behavioural control not only determines intention but also directly influences behaviour. This allows it to accommodate for situations when there are elements that are out of a user's control (e.g. lack of resources or to perform the action).

The three determinants of behaviour are in turn based on a set of *beliefs*. Beliefs are the *"subjective probability of a relation between the object of belief and some other object, value, concept or attribute"* (Fishbein & Ajzen, 1975). They are the judgements an individual makes about the world around him/her:

1. **Behavioural beliefs.** The consequences an individual attaches to carrying out the behaviour; it influences attitudes.
2. **Normative beliefs.** An individual's view of whether other people approve or disapprove of the behaviour. Subjective norm is formed on an individual's normative beliefs.
3. **Control beliefs.** The perceived presence or absence of resources. These beliefs are based on previous experience or second-hand information. Control beliefs influence an individual's perceived behavioural control.

3.3.3 Technology Acceptance Model

In his doctoral thesis, Davis (1985) outlined the *Technology Acceptance Model (TAM)*, which was an adaptation to the TRA, designed specifically to explain the adoption of information systems. According to the TAM, attitude was influenced by two particular belief level constructs about computer systems (Davis, Bagozzi, & Warshaw, 1989):

1. **Perceived usefulness.** An individual's subjective view that using the system will increase performance.
2. **Perceived ease of use.** An individual's perception of how hard/easy it is to use the system.

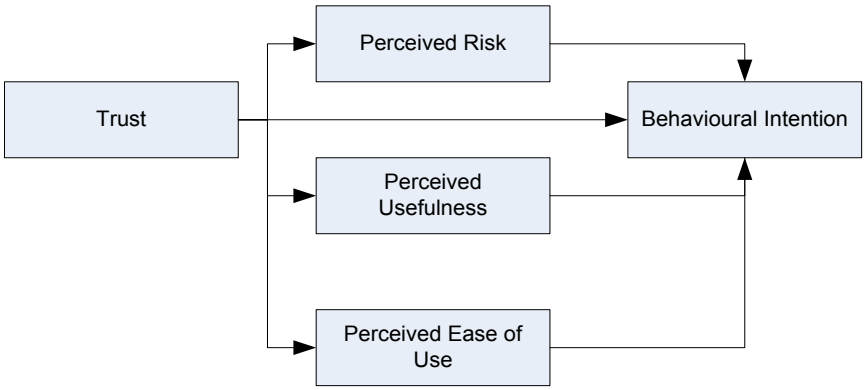


Figure 8 Technology Acceptance Model, with trust and risk factors (Pavlou, 2003)

Although not explored in this thesis, these two constructs are believed to be affected by various external variables, such as the visual design of the system, as well as the provision of system training and education. In expanding the use of the TAM into consumer acceptance of e-commerce websites, (Pavlou, 2003) integrated two more factors of interest to the research here:

1. **Perceived risk.** Individuals' perception of possible loss in carrying out an action.
2. **Trust.** Individuals' belief that the other party will act responsibly.

The study found that the inclusion of the trust and risk constructs greatly improved the explanatory power of the model; *perceived risk* was a factor that directly influenced behavioural intention; trust also influenced behavioural intention, but also had an impact on perceived risk, perceived usefulness, and ease of use.

3.3.3.1 McKnight's model of trust

Exploring adoption and behaviour within an e-commerce setting, McKnight et al. (2002) present a multidisciplinary model of trust. Similar to TAM, the TRA was used as a broad overall framework; the aim of the trust model was to develop a complete understanding of how individuals develop initial trust towards e-commerce websites.

Based on prior research, McKnight's trust model took a parsimonious version of the TRA, dropping the attitudinal constructs, positing that belief level constructs directly influence an individual's trusting intention to engage with a web-vendor. These trusting beliefs are framed as the trustor's perceptions of three web-vendor attributes (McKnight et al., 2002a):

1. **Competence.** The ability of the trustee to fulfil trustor's needs.
2. **Benevolence.** The trustee's general motivation to fulfil promise.
3. **Integrity.** Individuals' perceptions of the trustee's honesty.

The model further states that trusting beliefs are influenced by:

4. **Disposition to trust.** The trustor's personal tendency to trust/depend on others.
5. **Institution-based trust.** Trustor's belief that structural conditions are to ensure success (e.g. laws and technology infrastructure).

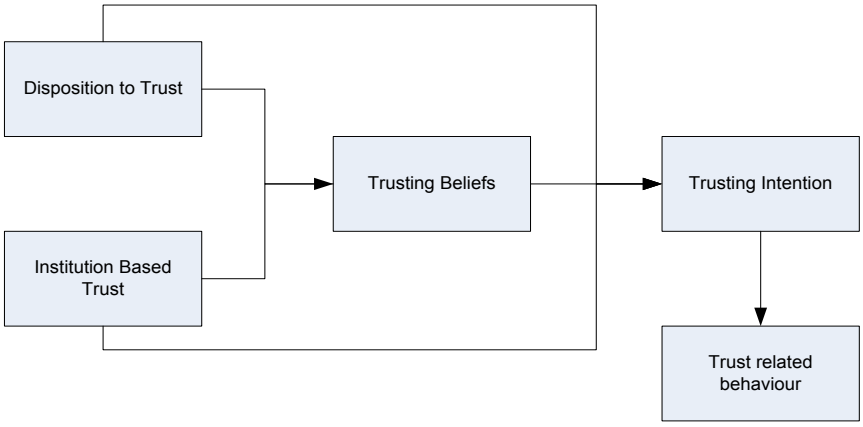


Figure 9 McKinght's Model of Trust

Similar to Pavlou (2003), McKnight, Choudhury, & Kacmar (2002b) further explored the effect of risk perceptions on behavioural intentions. Modelled as *perceived web risk*, this captures *"the extent to which a user believes it is unsafe to use the web or that negative consequences are possible"* (McKnight et al., 2002b). Together, the trust and risk were found to be significant predictors of behavioural intentions towards carrying out a trusting action.

3.3.3.2 Internet Users' Information Privacy Concerns: a causal model

Tying privacy concerns to the behavioural intention in e-commerce transactions, Malhotra, Kim, & Agarwal (2004), explored the effects of information collection and use on individuals' behavioural intentions. Drawing on *social contract theory*, as well as the information privacy dimensions (Smith et al., 1996), the study conceptualised a measure for *Internet Users' Information Privacy Concerns (IUIPC)* as a second order variable that was found to have an influence on the individual's *trusting belief* and *risk beliefs*. The IUIPC influences individuals' perception of the following factors:

1. **Collection.** The degree to which an individual is concerned about the amount of personal information collected to the perceived benefits.
2. **Control.** The individual's view of the amount of say that the individual has over his/her personal information.
3. **Awareness.** The degree to which an individual is concerned about his/her knowledge of an organisation's information privacy practices.

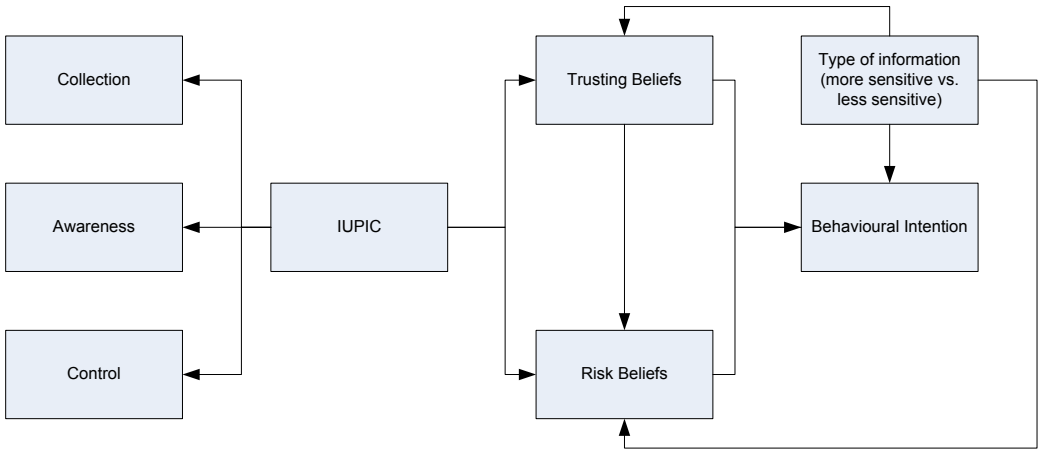


Figure 10 IUPIC model that links information type to behavioural intention

More interestingly for this thesis, Malhotra et al. (2004) also explored the effect that the *type of information* requested had on behavioural intentions. The study found that information type had a significant impact on individual perception and intentions; *"more sensitive information significantly decreased trusting beliefs, increased risk beliefs, and decreased intention"* (Malhotra et al., 2004).

3.3.4 Linking Trust to N-IDMS

The various e-Commerce based trust, risk, and adoption models have been applied to explore the adoption rates of new e-government services (for examples see Belanger & Carter, 2008; Lemuria Carter & Bélanger, 2005).

However, there has been little to no published studies that apply trust to N-IDMSs, such that Halperin & Backhouse (2008) states that "*trust, is a vital issue for this topic [identity] that requires theorizing and operationalizing to be studied within the context of identity*".

3.3.4.1 Trust, Risk, and eID

Studying individuals' perceptions of eID from citizens in the UK and Germany, (Halperin & Backhouse, 2012) have proposed a trust-risk model that is theorised to influence individuals' behavioural intentions to adopt a system.

Using open ended survey questions, which were analysed using Grounded Theory, Halperin and Backhouse put forward that intentions is influenced by individuals' risk perceptions:

1. **Information risks.** Risks associated with the handling and processing of personal information, as well as the technology used in such activities.
2. **Economical risk.** Individuals' cost-benefit assessment of the system.` This not only deals with individuals' personal economic gain/loss, but is also an individuals' assessment of public funds.
3. **Socio-Political risk.** Individuals' concern about the growth of government power, at the loss of citizen rights.

These risk perceptions would in turn be influenced by individuals trusting beliefs in the organisation:

4. **Competence.** Perception that the organisation will be able to keep the eID system secure.
5. **Integrity.** Perception that the organisation will use the identity information in a manner not agreed by individuals.
6. **Benevolence.** Perception of organisations underlying motives for introducing the system. Is the eID system designed to empower individuals, or to increase organisations' surveillance power?

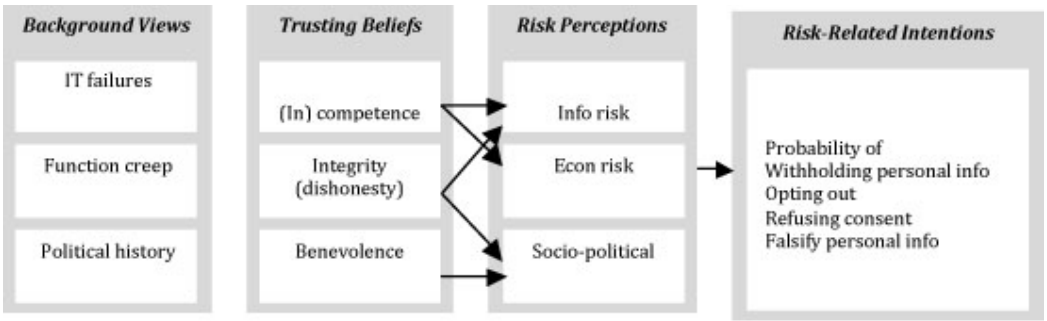


Figure 11 Halperin & Backhouse (2012) proposed trust model in eID

Furthermore, individuals trusting beliefs are formed on individual's background views. Background views refer to the role of past events or experiences involving the organisation, whereby negative events serve to lower individuals trusting beliefs in the organisation. Three types of background views were identified:

7. **IT failures.** Organisations past failed implementations of technology systems.
8. **Function creep.** Previous events where governments have authorised the use of personal information for other states purposes.
9. **Political history.** The past relationship between individual's rights and the organisation. For example, Halperin and Backhouse state that a history of totalitarianism is linked with doubts over governments' goodwill.

3.3.4.2 Li's model of Trust

Li (2004) developed and tested a comprehensive model of trust that predicts citizen's trust in N-IDMS. The new model is rooted in TRA and TPB. As such, Li's (2004) model predicts trusting behaviour through behavioural intention.

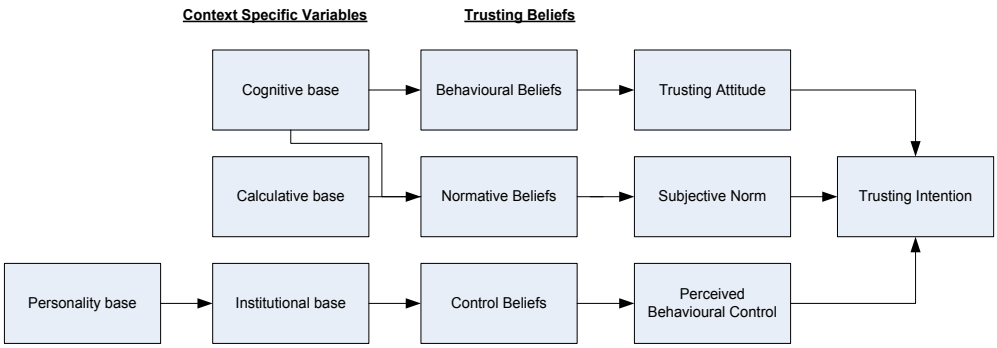


Figure 12 Li's Model of Trust in N-IDMS

Borrowing constructs from other models, such as McKnight's model of trust (Section 3.3.3.1), the aim of the research was to uncover the *context specific variables* that influence the trusting belief constructs; these constructs were not covered in the original TRA and TPB models. Li (2004) developed four context specific variables, termed *bases,* which are shown to influence beliefs:

1. **Personality base.** Individuals' general tendency to trust. The sub-constructs of the personality base are faith in competence, faith in benevolence, faith in integrity and trusting stance.

2. **Cognitive base.** Cues and impressions on the basis of which individuals form their trust; an individual's assessment of the object or system in question is dependent on its reputation, stereotypes, and people's illusion of control.
3. **Calculative base.** Individuals' perception of cost *vs*. benefit of carrying out the trusting behaviour.
4. **Institutional base.** The availability of structures that enhance trust. Situational normality and structural assurance will be used to represent this trusting base.

Through empirical research, Li (2004) established that the *cognitive base* determined behavioural and normative beliefs, the *calculative base* affected the normative beliefs, and the *institutional base* influenced an individual's perceived behavioural control. The *personality base* was found to influence the *institutional base* variable.

Li (2004) also found that mandatory systems increase trusting intentions. However, this should not be relied upon as a method to ensure adoption. It would be more beneficial for an organisation to increase positive attitudes, subjective norms, and perceived behavioural control which would make individuals want to use the system, thus ensuring that initial adoption turns into on-going use. For example, referring to further research of TAM within the workplace, Venkatesh & Davis (2000) found that mandatory systems increased individuals' subjective norms, and thus, intentions to use a system during the early stages of implementation (one to two months after implementation); however, the study also revealed that over time (three months after implementation) intention to use the system is not affected by these subjective norms and mandates of use.

3.3.5 Limitations of Current IDMS Trust Research

IDMSs create privacy concerns, affecting risk beliefs that require individuals to trust the implementing organisation; these risks arise from the unpredictability of negative outcomes. Trust mediates the risks, and thus both concepts are highly intertwined, so much so, that efforts to reduce privacy concerns can be seen as methods to induce trusting behaviour. In these cases, trust and risk should not be studied in isolation of one another.

While Li's (2004) trust model for N-IDMS is useful, it does not consider the risks that require it. Although the trust model does have a calculative base that may capture some of the risk involved, an examination of the questions used to explore this construct do not include any specific system variables; i.e. the model does not account for how the system design may affect individuals' perception of risk or trust.

Looking at the research conducted by Malhotra et al. (2004), we can see that the type of information has an impact on the overall trust beliefs, risk beliefs and behavioural intentions. Research to further bolster the strength of such models needs to further build on these elements, exploring how individual perceptions regarding the collection, storage and use of identity information affects the overall behavioural intentions. Therefore, it would be useful for IDMS trust research to explore how the system design itself can affect individuals' trust and risk perceptions, and hence their intention to accept these systems.

3.4 Culture

> *"Culture consists of the unwritten rules of the social game. It is the collective programming of the mind that distinguishes the members of one group or category of people from others"* (Hofstede, 2005).

This thesis also seeks to explore the effect of culture on individuals' behaviour around identity. The values individuals hold will influence their privacy risk perceptions and tolerance levels, thus affecting their behavioural intentions. The review reveals that, while some preliminary work has shown differences in the perception of IDMS between individuals from different countries, it has not been analysed within any formal cultural framework (Section 3.4.2.1).

Culture carries many meanings; in the context of this research, culture is defined as patterns across groups; this includes the *explicit* observable forms of culture, as well as the *implicit* thought patterns that are common to a group of people (Section 3.4.1). These explicit forms include the behaviours, rituals, and artefacts that can be recorded, while the implicit consists of a set of values that are internal to groups. Implicit culture refers to broad tendencies and preferences of groups to the world around them. An analysis of the two levels of culture reveals that the internal implicit patterns shape the outer explicit forms of culture-like behaviour.

The implicit, being the internal collective state of mind, dictates acceptable behaviour expected of individuals (Section 3.4.1.2). This has implications for the spread of culture within groups; faced with a situation, people in the same group expect other individuals to take a certain course of action as determined by the implicit values that they hold; this correct expected action taken then serves to reaffirms those implicit values.

Extending the concept of culture to groups of people across countries gives rise to the concept of a *national culture* (Section 3.4.2). Therefore, despite the heterogeneity that is present within countries, a national culture is believed to exist in which the people of a country share similar values. The impact that this has on national identity schemes may help to determine the success or failure of such systems. As such, this thesis will seek to make use of national culture to determine the influences that national culture has on the development of individual perceptions of N-IDMS.

3.4.1 What is Culture?

Culture is an all-pervasive force that shapes and exerts an influence on individuals' actions and behaviours. As Hickson & Pugh (1995) put it, culture *"shapes everything"*. The current era of globalization has highlighted the importance of culture and its effects; in a time when organisations are spread out across several continents, culture can be used as a tool to understand and possibly predict the possible ramifications. For example the rejection of N-IDMS by the general public in the UK (Section 2.2.2.2 and 2.3.2.1) may be partially attributed to national culture; in fact, the research here uncovers that the populations' individualistic values raise much concern regarding the potential erosion of freedoms caused by N-IDMS (see Section 6.5.2). However, despite the growing use of cultural studies, there is still much debate in the fields of anthropology, psychology and sociology as to what culture really is, and what impact it has on behaviour (McSweeney, 2002).

A source of confusion and controversy around the word is its varied use in everyday language (Dahl, 2004). On one hand, the phrase 'work culture' might refer to the work ethic within an organisation. However, when used to describe a person as 'cultured' the term takes on a new form, i.e. describing a highly educated individual. However, the one thread that is common to all interpretations is that culture isn't a physical manifestation. It is an abstract phenomenon, one that is so embedded in everyday life that it becomes hard to capture. Hall (1984) described it as an invisible mechanism that steers and controls our lives. As such, the far-reaching effects of culture have resulted in the term being adopted for use in several different fields to represent seemingly unrelated concepts.

At a basic level, culture can be defined as a shared system of values and patterns across groups of people. Compiling the various definitions of culture present at the time, Kroeber & Kluckhohn (1963) state that *"culture consists of patterns, explicit and implicit, of and for behaviour acquired and transmitted by symbols, constituting the distinctive achievements of human groups, including their embodiment in artefacts; the essential core of culture consists of traditional (i.e. historically derived and selected) ideas and especially their attached values; culture systems may, on the one hand, be considered as products of action, on the other, as conditional elements of future action."* *Explicit* in this definition refers to the observable forms of culture-like actions and behaviour. *Implicit* refers to thoughts and ideas about the world. Hofstede, 2005) refers to this implicit concept as *mental programming*.

3.4.1.1 The shape of culture

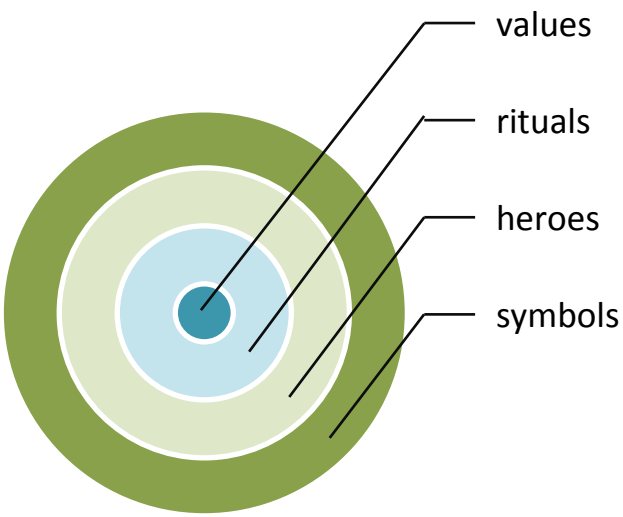


Figure 13 The onion-layer model of culture

The separation of culture into a two-tiered structure (the implicit and the explicit) is an important one, as it is the implicit shared values that influence the explicit actions. Hofstede (2001) elaborates on this structure through a layered model; here culture is shaped like an onion, with various layers, at the core of which lie shared group values. The explicit is further broken down into various layers, with each layer dependent on the layers below it. This model illustrates how the values at the core have an influence over the observable facets of culture.

Spencer-Oatey (2008) introduces some modifications to this model. While the core values remain unchanged, it is encircled not by rituals but by *beliefs, attitudes and conventions*. This is then followed by the concepts of *systems* and *institutions* and finally *artefacts, rituals, and behaviour*. The introduction of the second layer of attitudes and beliefs corresponds to another layer of the implicit culture that allows for the variation that might occur within a group. Individuals are unlikely to have exact attitudes, but are more likely to show *family resemblances*, which can be contributed to the unique personalities of each individual.

An individual's *mental programming* can be broken down into three different levels (Hofstede, 2001):

1. **The universal.** The most basic and applies to all human beings regardless of group membership (e.g. survival instinct, etc.).
2. **The collective.** The collective programming, which refers to the cultural influences.
3. **The individual.** The truly unique part of a person's mental state. This allows for individual personalities and can account for the heterogeneity in a group.

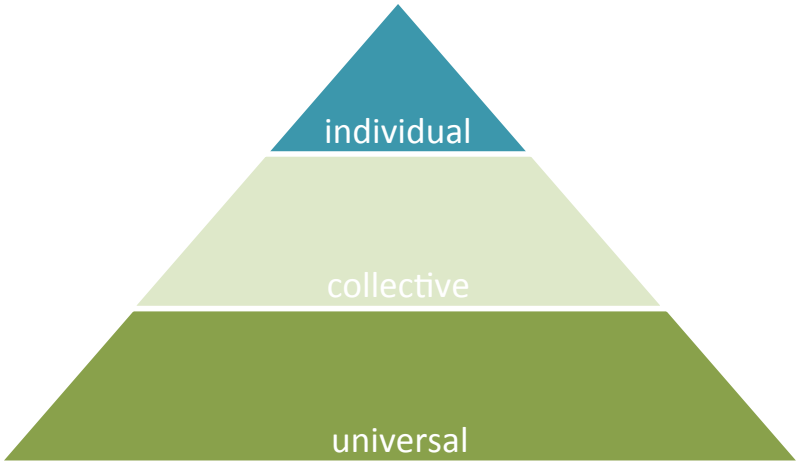


Figure 14 The levels of human programming. The universal, the collective, and the individual

3.4.1.2 The spread of culture

The implicit values shared among a group of individuals influence behaviour, which materialises as common explicit actions. Not only are these culturally driven actions common within the group, but they also become expected social behaviour. Triandis (1972) introduced the concept of a *subjective culture*, in which the mental programming is used as a means of deciphering the social environment. When interacting with other people, an individual perceives and assesses the situation through the values that he/she has internalized. As such, any action taken is influenced by his/her perception, and hence values. Observers of the situation holding the same cultural values would likely anticipate the individual's behaviour. Not only is a certain course of action anticipated, but it is also expected; culture acts as an invisible control mechanism (Hall, 1984). Once carried out, the action only serves to reaffirm the values. Therefore, in a way culture feeds on itself: it influences action, and is further reinforced by it.

This is in line with Hofstede (2005) view, in which the *"transfer of collective software [i.e. the shared cultural values] is a social phenomenon"*. Unlike the universal level of programming, which is believed to be largely hereditary, the collective level is learned (Hofstede, 2005); it is obtained from a very young age when individuals are exposed to the environment around them. Through observation of the habits and rituals of others around them, individuals absorb the messages and rules by which the particular society plays. This creates a *"system of permanent and transferable tendencies… which can be collectively orchestrated without an actual conductor"* (Bourdieu 1980 as quoted in Hofstede, 2001).

3.4.2 National Culture

Given the definition of culture as shared values within a group, how does one identify a culturally similar group? Wallerstein (1990) identifies cultural groups as those with some form of self-awareness, and some kind of organisation. Groups are said to have a culture if a *"statically significant relationship between group 'membership' and certain behaviour, or values"* exists (Wallerstein, 1990). As such, nations can be seen to possess a shared culture; individuals in the population are aware of being members of the group, and differences can be observed in the way different nationalities may act and behave.

However, we must also recognise that national culture is not the only culture within a nation. Individuals are members of many different groups. They possess multiple identities and assume various roles, each accompanied by their own set of cultural attributes; for example, there might be norms associated with a person's religion or work environment. Therefore, there is debate over the measurement of a national culture, given that differences may be encountered within such a large population (McSweeney, 2002). How can we identify and single out the preferences associated with national culture from the other subcultures that are present (or any culture national or otherwise)? There is compelling evidence that differences between populations in terms of preferences and values do exist, and that these differences can be measured (Hofstede, 2005; Schwartz, 1999; Trompenaars & Hampden-Turner, 1994).

One possible method of identifying culture would be through the observation of the outer layers, the explicit forms of culture. Through the observations of actions, behaviour and artefacts, one can slowly peel away the layers until arriving at the core. The other route to identifying the cultural values is by questioning the values themselves. This is the method that Hofstede, Schwartz and Fons Trompenaars subscribe to. Hofstede's work is easily the most prominent; though critics claim that his cultural measures are out-dated, unreliable, and contain too few dimensions too accurately capture national culture. However, these concerns are addressed by the large body of replications that support the Hofstede's original findings (Hofstede, 2005; Sondergaard, 1994). Furthermore, new dimensions have recently been added (Geert Hofstede, Minkov, & Vinken, 2008), keeping Hofstede's measures remain current, while capturing as much cultural diversity as possible. Thus, in this thesis, Hofstede's measures are favoured in exploring any cross-cultural differences.

Hofstede (2005) defines cultural values as *"broad tendencies to prefer certain states over others"*. He discovered nuances in cultural difference while conducting research for IBM looking into organisational culture. His initial study revealed four sets of values that capture differences in national culture; the four sets of values as defined by (Geert Hofstede et al., 2008) are:

1. **Power Distance.** *The extent to which the less powerful members of a society accept and expect that power is distributed unequally. A high value for this index represents a large amount of inequality that is both exerted from leaders and accepted by the followers.*

2. **Uncertainty Avoidance** *is the measure of society's tolerance for uncertainty and ambiguity. A high measure of this index is usually accompanied by strict laws and rules that minimise unstructured situations. Uncertainty accepting cultures on the other hand tend to be accepting of others' views and have as few rules as possible.*
3. **Individualism** *is the opposite of collectivism. Individualism stands for a society in which the ties between individuals are loose: a person is expected to look after himself or herself and his or her immediate family only. Collectivism stands for a society in which people are integrated from birth onwards into strong, cohesive in-groups, which continue to protect them throughout their life in exchange for unquestioning loyalty.*
4. **Masculinity** *is the opposite of femininity. Masculinity stands for a society in which social gender roles are clearly distinct: men are supposed to be assertive, tough, and focused on material success; women are supposed to be more modest, tender, and concerned with the quality of life. Femininity stands for a society in which social gender roles overlap: both men and women are supposed to be modest, tender, and concerned with the quality of life*

Later research investigating culture based on Hofstede's model identified another value (G Hofstede & Bond, 1988). This was followed by the discovery of two other values that were incorporated in to the framework (Van Vugt, Ronnie G.M.A. 2006 in Hofstede 2008). This brings the total number of cultural values to seven. The new values added are:

5. **Long-Term Orientation** *is the opposite of short-term orientation. Long-term orientation stands for a society that fosters virtues oriented towards future rewards, in particular adaptation, perseverance and thrift. Short-term orientation stands for a society that fosters virtues related to the past and present, in particular respect for tradition, preservation of "face", and fulfilling social obligations* (Hofstede & Bond, 1998).

6. **Indulgence** *stands for a society which allows relatively free gratification of some desires and feelings, especially those that have to do with leisure, merrymaking with friends, spending, consumption and sex. Its opposite pole, restraint, stands for a society that controls such gratification, and where people feel less able to enjoy their lives* **(**Van Vugt, 2006 in Hofstede 2008).
7. **Monumentalism** *stands for a society that rewards people who are, metaphorically speaking, like monuments: proud and unchangeable. Its opposite pole, self-effacement, stands for a society that rewards humility and flexibility. The monumentalism index will probably be negatively correlated with the long-term orientation index, but it includes aspects not covered by the latter* (Van Vugt 2006 in Hofstede 2008).

3.4.2.1 Impact of National Culture on IDMS

A review of the literature reveals that culture is a rich source of information about groups of people and their preferences. The values that groups possess form the core of any culture that then influence the beliefs, attitudes, behaviours, and actions. Therefore, culture can be a valuable and powerful tool that can be used to predict people's reactions. From management to various fields of human-computer interaction, the implications are so widespread that many researchers from diverse fields have attempted to utilise culture to explain behaviour.

As such, it is useful to consider culture in determining the acceptability of N-IDMSs. If the designs of such systems go against the core values of the national culture, then it is likely for the system to be rejected. While there has been some work done in the area of culture, trust and privacy, there have not been any studies that specifically explore the cultural effects on IDMSs; research should attempt to fill this gap, and explore the effects of national culture within the context of IDMS.

3.4.2.2 Privacy and the influence of culture

The sharing of information can be seen as a social action, and therefore may be affected by the norms and culture present within that society. The nature of information and hence its sensitivity is determined by the structure of societies in place. For example, a closely-knit community might not regard a piece of information as sensitive; on the other hand, a fragmented setting might highly value the privacy of the same information. In the same way, a highly bureaucratic society might see the government as a non-threatening receiver of information, while an oppressed society might view it negatively.

There has been some research that attempt to link informational privacy and culture. Milberg, Burke, Smith, & Kallman (1995) first attempt failed to establish any link whatsoever between informational privacy concern and culture, but did uncover the influence of national culture on the level of government involvement in privacy issues. Using Hofstede (2001) *Cultural Values Measures*, the second study conducted by Milberg, Smith, & Burke (2000) revealed a positive correlation between power distance, individualism and masculinity and privacy concerns. Uncertainty avoidance had a negative impact on privacy concerns. However, a separate study by Bellman, Johnson, Kobrin, & Lohse (2004) failed to corroborate these findings, and instead discovered that power distance, individualism and masculinity had a negative influence on privacy concerns.

The discrepancy in the results of the two studies may be accounted for by the different statistical methods; when applying the same statistical methods as Milberg et al. (2000), Bellman et al. (2004) found a similarity, in that uncertainty avoidance was negatively correlated with privacy concerns. Another source of discrepancy may be attributed to the differing levels of analysis; Milberg et al. (2000) looked at correlations between cultural values and overall informational privacy concerns, while Bellman et al. (2004) analysed correlations with each individual information privacy construct (i.e. collection, improper access, errors, and unauthorised use). Lastly, the two studies look at privacy concerns in two different contexts; Milberg et al. (2000) framed the privacy concerns relating to organisations, while Bellman et al. (2004) focused on privacy concerns in websites. Therefore, the results of these studies do not appear to be comparable until an agreed study protocol is used across the different studies.

3.4.2.3 Linking trust to culture

The literature linking culture to trust is less developed than that available on privacy. There is a lack of studies that investigate the effects of national culture on the development of trust. In a call to explore the area, Doney, Cannon, & Mullen (1998) have theorised the effect of culture on trust, but have not explored it further. Some evidence for the effect of culture on trust comes from Backhouse & Halperin (2007) survey of European citizens' trust of identity systems.

Their results indicate that citizens' in Central and Eastern Europe had largely positive attitudes towards N-IDMSs and authorities, when compared to the negative responses obtained from the UK, Ireland, Germany, Austria, Finland, and Scandinavian countries. The findings were not explored in the context of any cultural measures such as those of Hofstede (2005), but indicate that there might be a possible effect of national culture on the development of trust.

3.5 Organisations and N-IDMS

Organisations implement an IDMS to fulfil a particular purpose. The design of a system will reflect the goals that the organisation is trying to achieve, thus making the organisation a critical part of this research (Section 3.5.1.1).

Looking specifically at N-IDMS, the organisation in question is the government agency that is tasked with the planning, implementation, and management of the system. There is little published research that covers how organisational identity requirements and purpose shapes the design of an identity system. Within the computer science literature, *Identity Management Architectures (IDMA)* have been proposed that are either focused on specific technological details, or detail a high-level overview of IDMS workflows and processes; in either case IDMAs do not capture or describe how organisational identity requirements and purpose actually influences the implementation details (Section 3.5.2.1).

There is also available research that focuses on the public policy debates about N-IDMS; of interest to this thesis, current investigations have uncovered a *short-circuiting* of these identity policy debates, by reducing discussions to technological aspects, without suitable assessment of fit-for-purpose (Section 3.5.2.2 and 3.5.2.3). These debates focus on the theoretical evidence presented by the government agency, which do not fully explore the complexities and effectiveness of identity technology in its implementation context.

Further research should attempt to address this problem by investigating how the purpose and requirements of an organisation shape the planning and design of implementation of an IDMS (Section 3.5.3).

3.5.1 Investigating Organisations

Identity pervades all levels of social interactions, and is either managed by individuals or organisations; on a personal level, identity is managed by each individual, who draws upon his/her mental constructions and memories to construct identities for each person he/she encounters; however, on a larger scale, officially recognised forms of identities are managed by organisations that ensure the validity of registered identities.

The conditions under which these managed identities can be used are defined by the organisation; more accurately, organisations implement and design identity systems to fulfil a particular purpose. Therefore, the implementing organisation's requirements and expectations behind identity become an important component in the research of IDMS. As this research largely deals with N-IDMS, the organisation in question is the government or the specific government agency tasked with the planning, implementation, and running of an N-IDMS.

3.5.1.1 Purpose of the IDMS

The purpose for which a system is implemented will influence its design, so that it can best achieve the goals set out for it. Having clearly established goals for an IDMS will aid in identifying the individuals that will be enrolled, what personal information will be collected, as well as identifying who will be able to access the identity, and what they can use it for. *"Decisions made at this level will also have ramifications for the technological underpinnings of the system, including what levels and kinds of system security will be required"* (Kent & Millett, 2002).

Specifically considering N-IDMS, purpose is partly defined by the context of the situation in which it is introduced; objectives of the system are driven by the unique requirements of each country. While the overall aims across different countries may be the same (e.g. reduce terrorism or tackle immigration), the manner in which it is deployed might not be. Each system needs to be tailored to each country by accounting for population size, current immigration procedures, laws and a variety of other constructs. A statement that clearly defines the purpose of an N-IDMS system will allow the formulation of a strategy, and an assessment of that strategy, to be made in relation to its unique implementation conditions.

It should be noted that an N-IDMS can have more than one purpose. We have already identified early on (Section 1.2 and 1.3) that proponents of N-IDMS see identity as a silver bullet, being able to increase government efficiency, while also reducing organized crime, battling terrorism, and tackling benefit fraud; all of which have been arguments put forward by the UK in its recently scrapped pursuit of an N-IDMS (Section 2.3.2.1 and Section 7.2.2). Therefore, organizations must be clear about the entire purpose(s) of the identity system, and everything that it will be used for.

3.5.2 Short-comings of current approaches

Recognising that IDMS should be designed to fit the purpose of the system, current approaches do not account for it. Traditional identity literature that address (Section 3.5.2.1 and Section 3.5.2.3) organisations' concerns over the implementation of an IDMS tend to focus on the basic identity lifecycle and identity architectures as identified in Section 3.1.2.1. Similar to the pattern identified within the identity, privacy, and trust literature, organisations still view identity simply as an authentication mechanism. As such, the literature does not account for the strategic value of identity to the organisation, and its influence on the success or failure of an IDMS implementation; *"most of this research [on N-IDMS] deals with individual identity management, or with identity management within organisations. There is not much discussion for similar features with regard to official identities of citizens on the national level"* (Kubicek, 2010).

3.5.2.1 Identity Management Architecture (IDMA)

An IDMA is a *"set of processes, workflow, framework, standards, and policies that defines and describes a system of Identity Management"* (White, 2008); it is a blueprint that describes all the components of an IDMS, thus providing organisations with a structure and roadmap for the design and implementation of an identity system.

In his doctoral thesis, White (2008) developed an IDMA that was technology agnostic, while integrating higher order strategic aims; this is a significant departure from traditional architectures that focused on technical security aspects of an IDMS (Windley, 2005). Analysing several federated identity systems implemented by the Australian government, the proposed architecture consisted of several different frameworks as illustrated in Figure 4 (see Section 3.1.2.1).

While White's (2008) architecture is a step forward from the security technology perspective, it is not without its shortcomings. First of all, despite *"integrating the organisations strategic aims"*, the high level view of the IDMA means that it is absent of any specific details regarding the actual considerations that affect implementation; what are the actual factors that the organisation must consider to ensure a system that is fit-for-purpose?

Secondly, while it is suggested that the IDMA can be used to design citizen side N-IDMS, it is highly limited to a Type 1 IDMS configuration (Section 3.1.2.1). The architecture was developed within the context of identity as an authenticator to access a resource. However, as described earlier (Section 3.1.4), identity is no longer just used as a mechanism to access the resource, but has itself becomes the resource that is being accessed and used by the organisation. Therefore, coupled with the high level view of the architecture, White (2008) briefly describes that the construction of identity (i.e. the choice of identity information, its collection, storage, etc.) as a function of the Human Resource department.

Finally, a result of the high level Type 1 view of the IDMA, the privacy management framework takes a very functional view, looking at integrating typical *"enterprise privacy policies"* (White, 2008). As uncovered in the privacy literature review, typical privacy polices takes a functional confidentiality approach, and that future privacy work needs to stretch towards the greater implications on the lived experience (Section 3.2.5).

3.5.2.2 Framework for the Path of New N-IDMS

While White (2008) focused on distilling common attributes of IDMS into an architecture, Kubicek (2010) took a different approach, focusing on the differences between N-IDMSs in Europe, hoping to *"understand the differences between national eIDMS in other European countries, and assess the scope and magnitude of changes in the citizen-government relation"*.

As a background, several European governments are in various stages of the planning, implementation, and distribution of citizen *electronic identities (eID)* to support their e-government and e-commerce agendas. Different countries have each chosen different approaches, implementing measures that they believe best fit their needs and situations. It is within this context of exploring inter-operability of the different eIDs schemes that a framework is developed to explain the differences noted across different N-IDMS (Kubicek, 2010).

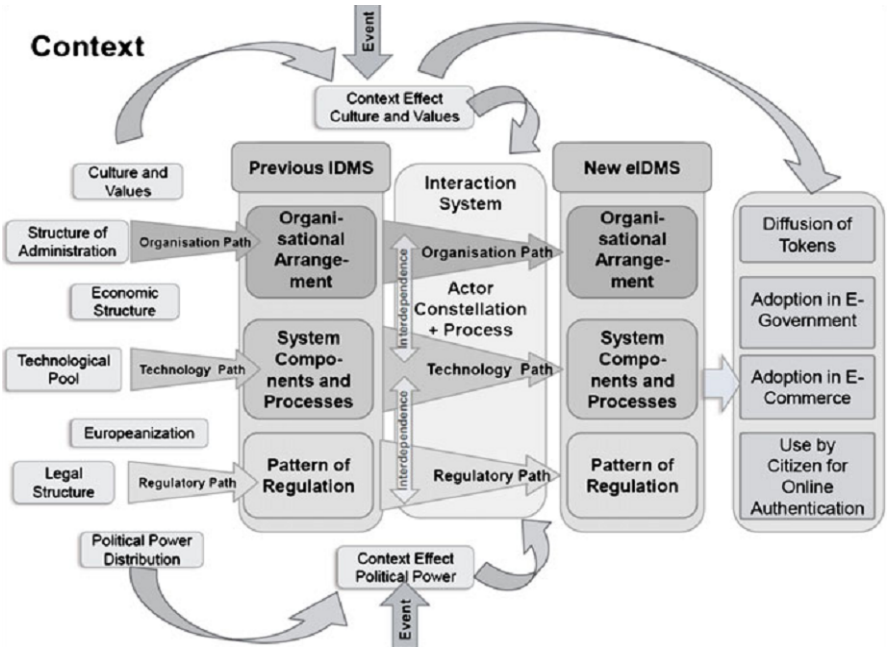


Figure 15 Kubicke's (2010) path analysis for eIDMS

Using a mixture of *path analysis, institutional actor theory and policy field analysis*, the study focused on eight different countries (Austria, Belgium, Estonia, Finland, Germany, Italy, Portugal, and Spain). The research found that the current organisational, technological, and regulatory arrangements have a very strong tendency to be brought forward into the new system. *"Path changes and path creation have to be explained, while path continuation is the default assumption"* (Kubicek & Noack, 2010b). For example, Sweden has typically relied on other organisations for identities, and chose to outsource the administration of its new N-IDMS to banking consortiums. In contrast, governments, like Germany, that have typically kept control of identity tend seek to implement government-controlled and managed identities. Cultural attitudes and norms also have an effect, where privacy sensitive countries with stronger regulations tend to have higher security requirements, and privacy legislations when implementing the new systems.

The research has also found that identity discussions, despite being a multi-field policy effort, fail to cater for other policy actors that they would like to interact with. As a result, there is low uptake of the identity by other public and private agencies, as the lack of co-ordination has resulted in low level of perceived benefit (Kubicek & Noack, 2010b). With regards to citizen-government relationships, the research has found that eIDs are not appropriate or effective solutions to addressing an individual's security and safety concerns. Kubicek & Noack (2010b) argue that these problems occur because *"policy makers following the advice of technical experts reduced the societal problem to a technical problem"*. Technological concerns and trust were typically reduced to discussions and precautions around technical security, instead of the identity system itself in relation to the purpose.

Finally, the researchers found no compelling evidence that links eIDs to changes in the citizen-government relationship. The privacy fears brought about by the digitalisation of identity and its impacts on the citizen were non-existent, as to *"citizens it is still considered and used as means for interpersonal authentication"* (Kubicek & Noack, 2010a).

However, while the study uncovers many dependencies, like White's (2008) IDMA, the study is limited towards Type 1 IDMS (Section 3.1.2.1). Little discussion is given towards the suitability of identity information and technologies being implemented. As a result it doesn't accurately explain for the low take up of government eIDs experienced in most of the countries investigated. Furthermore, this explains the lack of privacy concerns raised by citizens, who are not consulted about the strategic use of identity by the organisation; Kubicek & Noack (2010b) themselves admit that *"privacy concerns addressing the exchange of person-related data between different government back offices are without any doubt justified, but they are not influenced by the eIDMS for online authentication in the front offices. Rather front office and back office processes are quite independent with regard to privacy intrusion and provisions"*. Research needs to focus on the broader views of IDMS; to focus on identity on the strategic aims of the organisations, its use of identity to fulfil those aims, and thus the lived experience and perceptions of individuals with respect to the new approach.

3.5.2.3 Developing New Identity Policies

In investigating the role of policies in the development and success of new systems, Kubicek & Noack (2010b) point out the multidisciplinary nature of identity policy, highlighting the lack of interaction between the implementing organisation and other important actors, as well as the reductive approach of diminishing issues to pure technological discussion. Whitley & Hosein (2010) go on to explore these issues with the aim of developing effective identity policies that address various concerns.

Taking a broader view, Whitley & Hosein (2010) state that comprehensive identity policies *"involve creating or adopting schemes for the collection and processing of individual-specific data that will be shared across services, both within and beyond government, often for a variety of purposes"*. As with Kubicek & Noack (2010b), the authors highlight the delicate nature of identity policies that cut across various public and private policy drivers. This is further complicated by the technological aspects of an identity system; identity technology is commonly seen as a solution, but itself introduces new questions into the policy debates that are ignored, and thus can undermine the effectiveness of the identity solution.

Examining the recently abolished UK identity card system, Whitley & Hosein, (2010) conclude that governments attempt to manipulate and control the conversation by *short-circuiting* identity policy debates through the use of:

1. **International obligations.** These are used as an excuse to implement new technologies without deliberation. It creates a risk where policies are never adequately deliberated at any level, each level presuming that the other levels will or have done it.
2. **Technology and facts.** There is a separation of scientific fact from social action. It ignores perplexities of claims, not accepting of alternative knowledge claims, especially with policies that need to use science, in which there is no consensus within the scientific community.
3. **Language ambiguity.** The use of vague language to escape proper scrutiny.

Whitley & Hosein (2010) suggest that effective identity policies should be led by clear goals that facilitate responsive, reliable, and relevant development of technology, and limit abuse. The N-IDMS should also be proportionate and transparent, serving the individual and private sectors alike.

These recommendations are also reflected by Kent & Millett (2002), who state that identity policies need to address several questions, which will drive the identity technology considerations and final N-IDMS implementation:

1. **Purpose of the system?**
2. **Scope of the population?**
3. **Scope of the data?**
4. **Who would be the users?**
5. **What type of uses would be allowed?**
6. **Is participation voluntary or mandatory?**
7. **What legal structures would protect the system's integrity?**

3.5.3 Further Research

The currently available literature on organisations and N-IDMS has focused on high-level policy considerations, pointing out that a clear purpose will be determinant to implementing a successful system; a clear goal will influence the technological choices, and structure of the final identity system.

While Kubicek (2010) has developed a framework detailing the influences of external forces on the organisations plans on the N-IDMS, research could further benefit from a closer investigation into the decision making process that influences the specific identity technologies. Expanding on the knowledge base presented here, and its focus on purpose, research should investigate how particular organisational requirements may have an impact on the identity technologies, the information required to construct identity, and the structure of the final system.

Developing an in-depth framework that focuses on the identity system and the technologies or information required would provide a more accessible tool for system designers and researchers, helping to alleviate some of the problems caused by the technology and ambiguity in short-circuiting identity policy debates.

3.6 Chapter Summary

This chapter reviewed literature from the related fields of identity, trust, privacy, and culture; as well as an examination of organisations approach towards implementing N-IDMS. In so doing the thesis identifies gaps within the field that this research investigates.

Beginning with the concept of identity itself, the review has found that current definitions are limited by the traditional focus on Type 1 IDMS; identity is largely seen as a static object that is used as a security mechanism to gain access to resources. Driven by this purely functional concept of identity, current human-centric identity approaches typically focus on ease of use, merely treating individual's functional pieces within the system; for example, federated identity attempts to reduce barriers to sign up and information sharing.

Reflecting, or perhaps as a result of the shallow view of identity, the current privacy literature focuses on similarly narrow view of information privacy. Developments within in the field have traditionally focused on the issues of confidentially and data minimisation. Meanwhile, N-IDMS trust research is largely absent of individuals' perception of risk presented by an identity system.

Therefore, further research undertaken needs to consider a broader view of identity that reflects the real world. Identity systems have grown to become hybrid systems that not only control access to resources, but are used in a strategic manner to inform organisational decisions and interactions with an individual (Type 2 IDMS); this could range from simply providing individuals with personalised services, to tracking suspected terrorists.

This is the stance with which the thesis approaches the problem. In so doing, the research aims to fill the gaps taken by the traditional IDMS research. In terms of privacy, this means investigating the consequences of identity beyond that of the informational privacy; i.e. the research moves from the concepts of confidentiality and data minimisation towards the actual impacts of identity on individuals' lived experience. Similarly the research will take a broader view of the trust research, focusing on how the design of the system affects individuals' perceived risks, and hence its impact on the intention to adopt IDMSs.

This thesis also seeks to further augment the exploration of perceived risk and behavioural intention through an investigation of culture, which is an all-pervasive influence that shapes a populations behaviour and expectations. Thus, in the context of N-IDMS, national culture may explain for differences in the reaction of populations across different countries. While there has been some work done in the area of *culture*, *trust and privacy*, they have not been specifically explored within the context of identity systems; this research attempts to fill this gap, and explore how culture can affect the implementation and acceptance of IDMSs.

Finally, the thesis also recognises the organisation as an important stakeholder that shapes the implementation of an IDMS. Of prime importance is ensuring that the system design reflects the organisations purpose for implementing an IDMS. However, again current research has shown that identity is commonly seen as a security mechanism (i.e. Type 1 IDMS), thus ignoring the overall lived experience. Further exacerbating the situation, organisations typically short-circuit N-IDMS policy debates, refusing to entertain discussion or alternative views to ensure the proposed identity system is actually fit-for-purpose. Research should not be deterred by this fact, and therefore this thesis investigates the organisational requirements that shape IDMS, and thus guide the implementation to ensure a suitable system is implemented.

Chapter 4: Methodology

This thesis explores the relationship between individuals, organisations, and N-IDMS (Section 5.1). The research is exploratory, seeking to create a better understanding through empirical studies, utilising various methods to collect and analyse qualitative and quantitative data (Section 5.2.3).

The research was conducted in three separate studies; a system, an individual study, and an organisation centred studies (Section 4.3). Using historiography to collect second-hand accounts around past and present N-IDMS, the system study aimed to identify themes that capture the practical design aspects of N-IDMSs, and how these can impact everyday life (Section 4.3.4).

The individual and organisational studies, guided by an overall case study approach, investigated the implementation of N-IDMSs in Brunei, India, and the United Kingdom (Section 4.3.1). The individual study made use of focus groups to identify individual perceptions of N-IDMSs (Section 4.3.2.1), while the organisation study investigated the intentions in implementing N-IDMS using material collected from official documents and interviews (Section 4.3.3). Both areas of investigation made use of grounded theory to develop narratives and theory directly from the data.

The individual study also investigated the effect of culture on individual perceptions. This was done using Hofstede's cultural values (Section 4.3.2.3).

Finally, the thesis made use of triangulation to bring all the data together into a single coherent model, and also acted as a tool for validation and verification (Section 4.4).

4.1 Research Question and Direction

This thesis explores a human-centred approach to IDMS, focusing specifically on N-IDMS. A review of the identity literature has revealed that identity is typically seen as a functional access mechanism to security systems (Section 3.2 and 3.3). Meanwhile, a review of current research on organisations and IDMS reveals the importance of broader policy considerations, ensuring the IDMS and technology chosen is fit for purpose (Section 3.5.3).

Considering the gaps identified in the literature review (Section 3.1.4, 3.2.5, 3.3.5, 3.5.3), this thesis seeks to augment the field by answering the following question:

> *What are the human factors that influence identity, and how does it affect the development, implementation, and use of Identity Management Systems?*

4.2 Research Methods in Human Computer Interaction

To answer the above question, the research needed to identify and employ the appropriate methods of investigation. A review of the *Human Computer Interaction (HCI)* field uncovered a growing body of research methods that pulls in expertise from many disciplines.

Early HCI research were typically experimental studies that examined individuals' interaction with technology. These lab studies were focused on collecting objective performance measurements (e.g. task completion, time taken, etc.), as well as some subjective feedback on user satisfaction. This approach has now evolved to include advanced performance measures such as eye tracking, as well as objective measures of user-cost through the measurement of physiological indicators like stress.

However, these types of experimental lab studies are not suited to the investigation of complex ill-defined socio-technical phenomena (Anne Adams, Lunt, & Cairns, 2008). HCI research is highly contextual, driven by issues of user group, task, and context of interaction. Thus lab studies cannot be carried out in situations where these issues are not fully understood; i.e. the phenomena under investigation is not been fully defined. As Sasse (1997) states, *"HCI phenomena which have not been sufficiently well described and understood should not be expressed as formalisms and investigated by methods of scientific experimentation; instead, exploratory research is required to obtain precise descriptions as a basis for further research"*.

As the issue of human-centred identity is one that is not fully understood, this thesis does not seek to test some preconceived theory in structured lab experiments, but instead aims develop theory to better define and understand the phenomenon under investigation. This calls for an exploratory investigation that departs from using the traditional HCI quantitative approach, and draws more upon the qualitative domain of social-based investigations.

In order to fully appreciate the differences the quantitative and qualitative approaches, it would be beneficial to briefly review the two main research stances, positivism and constructivism, and how these can influence the choice of methods that researchers subscribe to.

4.2.1 Positivism and Quantitative Methods

Positivism is a philosophy of science that is driven by the belief that there is a single reality (Tashakkori & Teddlie, 1998). Positivists aim to achieve a purely objective and value free line of inquiry, focusing purely on the observable and measurable facts. The *naïve realism* and *objectivist assumption* of the positivist stance also implies that knowledge is easily generalizable across different contexts (Denzin & Lincoln, 1998). As such, positivists work under the assumption that one can determine *"how things really are" and "how things really work"* (Denzin & Lincoln, 1998). It is explanatory in nature, seeking to establish links of causality.

Driven by their ontological and epistemological views, positivists make use of experimental and scientific approaches. Armed with hypotheses, research makes use of quantitative methods, i.e. numerical based methods (King, Keohane, & Verba, 1994; Punch, 1998). The use of numbers provides the objectivity that underlies positivism in that researchers are presented with a set of unchanging numerical figures that has a uniform value to each and every researcher. However, not all data in the real world naturally assumes a numerical form; researchers enumerate this data by either employing techniques that involve counting or scales.

In trying to explore casual connections, the design of quantitative research must identify the variables that will be measured, of which there are three types; the *independent variable*, the *dependent variable* and the *control variable*. The independent variable is the variable that is theorised to cause fluctuations in the dependent variable. Control variables can also have an effect on the dependent variable; however, unlike the independent variable, researchers aim to partially or completely eliminate the influence of control variables.

The common tools for quantitative research are the use of questionnaires and surveys. Theory is generated *a priori*, implying that this form of research is suited for theory verification rather than theory generation. Clear themes, well-formed research questions, and complete research frameworks are essential for this purpose. Statistical methods are used to analyse the data gathered to prove the hypothesis that was been put forward.

4.2.2 Constructivism and Qualitative Methods

Constructivism, and its derivatives, assumes a stance that is diametrically opposite to that of positivism. The ontological and epistemological beliefs of constructivists were developed in response to the positivist point of view (Tashakkori & Teddlie, 1998). Constructivists believe that there are many different versions of realities; there is no one truth, as truth is constructed on the basis of ones experiences, which varies between individuals; research sought to identify the subjective experiences. The relativist assumptions and the subjective values of all participants naturally implied that generalizations from the particular were impossible; constructivists seek to understand the uniqueness of each context. It is exploratory in nature, as opposed to the explanatory positivist approach.

Constructivists reject quantitative methods, and make use of qualitative methods that develop understanding not through numbers but through words, behaviour, and their meanings (Corbin & Strauss, 1990). They focus on the use of non-statistical methods as a means of analysing data collected through a variety of techniques; these can include interviews, observations, documentation notes, and personal experience (Punch, 1998). Qualitative methods can be applied for many different purposes; they can be used to infer causal links, or to describe certain situations, as well as to develop or to verify theory. Whatever the case, the methods aim to develop a holistic view of the situation being studied, typically involving prolonged contact (Punch, 1998).

Unlike quantitative research, qualitative methods are diverse in terms of the techniques used to collect and analyse data. Additionally, studies of this nature tend to be relatively unstructured; research questions are vague, and the design of the inquiry process is developed as research is being conducted. Therefore, research tends to be an unfolding process that is loosely guided by general questions.

4.2.3 Pragmatism and Mixed Methods

While the various paradigms along with their respective quantitative and qualitative methods appear to be incompatible, many researchers today have advocated the complimentary use of both research methods, stating that the differences have been overdrawn by *purists* (Tashakkori & Teddlie, 1998). Pragmatists are aligned with the positivists, in the sense that they accept the existence of a single reality independent of our influence (Tashakkori & Teddlie, 1998). However, similar to the constructivists, pragmatists argue that one can never truly discover this truth, and that any explanation of the reality is interpreted. Pragmatist research is driven by a normative concept of truth, seeking to find the explanation or theory that works best, and realising that *"claims cannot be totally abstracted from contingent beliefs, interests and projects"* (Tashakkori & Teddlie, 1998).

Pragmatists are not aligned with one particular method. Instead, research strategy driven by the research question, i.e. the method for data collection and analysis is determined by the type of data that best answers the research question. Pragmatists make use of both quantitative and qualitative strategies; this mixed-method approach, can be broken down into three main categories (Tashakkori & Teddlie, 1998):

1. **Equivalent status designs.** Research places equal importance on both quantitative and qualitative methods.
2. **Dominant/less dominant designs.** Research is conducted using a dominant paradigm, supported by a small study using an alternative methodology.
3. **Multilevel use designs.** Various types of data are collected using different methodologies. All the data is collected together and analysed.

4.3 Research Approach

Ideally, the research conducted here would have investigated the human factors by building on existing knowledge that is already available in the field. However, current research into 'human-centred' IDMS is largely theoretical solutions that fail to fully capture the complexity of human behaviour (Section 3.1.4, 3.2.5, 3.3.5). A holistic approach is required to identify and assimilate the human factors that can affect the implementation of an IDMS.

Coupled with the fact that the concept of identity is highly dependent on the context of use, an exploratory approach is required to validate and extend the present body of research on the subject matter. Therefore, this research takes a pragmatic approach to the problem; it uses mixed-methods, dominated by qualitative studies, and where possible, is supported by quantitative methods.

The research conducted here was approached from three different perspectives and studies:

1. **System study.** Recognises the IDMS system itself as a key element within the ecosystem. The line of inquiry seeks to identify how a system implementation influences the social impacts that arise.
2. **Individual study.** This perspective seeks to discover how citizens think about and assess an IDMS. It seeks to explore the concerns that citizens have when confronted with an identity system.
3. **Organisation study.** Looks at organisations identity requirements, and how that influences the design and implementation of the identity system.

Each study utilised different techniques and methods that were best suited to the differing lines of enquiry. In order to fully explore the cultural influences of individual behaviour, as well as to maximise differences and similarities between organisations, the individual and organisational studies were further broken down into three separate case studies.

The following sections provide a general overview of the main methods used to explore each perspective. They also provide a general overview of the inquiry strategy used, leaving the specific application details to the later chapters that cover each of the three studies.

4.3.1 Case Study Research

Case study research is defined as *"an approach capable of examining a simple or complex phenomenon, with unit of analysis varying from single individuals to large corporations and businesses; it entails using a variety of lines of action in its data-gathering segments, and can meaningfully make use of and contribute to the application of theory"* (Berg, 2001). It is a systematic investigation of a phenomenon through one or more illustrative cases.

In the past, the usefulness of case studies has been questioned, whereby conventional wisdom believes that the findings uncovered cannot be generalised beyond the specific case(s) studied. However, Flyvbjerg (2006) who is an influential figure in the use of case studies has addressed the 5 common misunderstandings that underpins the erroneous conventional views:

1. **Theoretical knowledge is more valuable than concrete practical knowledge.** Working within the sociological domain, Flyvberg argues that one cannot find universal predictive theories when dealing with human affairs. Instead case studies and its closeness to real life aids in the development of nuanced view of reality.
2. **Generalisations cannot be made on the basis of a single case.** This point is countered by the use a *critical case*, where by theory generated under extreme conditions implies that it would hold under normal conditions. Alternatively a single case study can be useful for falsification, i.e. *black swans*.

3. **Case study is not suitable for hypothesis testing or theory building.** This misconception is built on the previous misconception, and therefore acceptance that generalisations can be made implies that case studies are useful for hypothesis and theory building. In fact, the deep study of multiple *extreme cases* that have *maximum variance* can aid in the generation of richer hypotheses and theories.
4. **The case study contains bias towards verification.** Experience in the case study approach has revealed that researchers are typically forced to reconsider their preconceptions, thus falsifying their original stance, and eliminating bias.
5. **Difficult to summarise and develop general propositions.** In this case, Flyvberg agrees that it is difficult to summarise case studies. However he goes on to state that good studies should be read as a narrative in its entirety, a *case story* is the result itself, and the contextual richness can prove to be better for policy intervention.

Therefore, as opposed to the old conventional wisdom, case studies can in fact be used for theory generation, providing a deep, *thick*, and generalizable understanding of the phenomena of interest.

The research here made use three main case studies, where the cases were chosen so as to reflect similar goals, i.e. the implementation of an N-IDMS that involved the enrolment of all citizens, and the provision of a unique national id number per citizen. However, each case was also unique in terms of the stage of implementation, levels of public acceptance, as well as integration within the country; this variance between the cases helps in the generation of rich theory as a large range of actors and experiences are captured and analysed (Flyvbjerg, 2006). The cases that were chosen for investigation are:

1. **United Kingdom.** The UK government has recently decommissioned its planned N-IDMS, and has now invalidated the identity cards that were produced; at the time the research here began, the system was just being implemented. Its initial introduction was met with much resistance. The UK government had high expectations of the system, stating that it would help in the battle against crime, immigration and terrorism.

2. **Brunei Darussalam.** The government introduced a digital smart card in 2000, which served as a replacement of the previous paper-based identification scheme. Although the digital N-IDMS has been around for eleven years, extended use of the card has been limited. Its main function is to identify citizens when required; recent new functionality allows the smart card to be used as an access card to certain benefit information, as well as being used as a frequent traveller card.
3. **India has faced little if any public opposition to its plans for an N-IDMS.** It is currently in the process of implementing the system, and enrolling citizens. When completed, it will be the largest N-IDMS system in the world. It also differs from the other systems in that it aims to provide a unique identity number for every person, but not necessarily provide them with an identity card.

These three cases formed the structure by which the individual and organisational studies were conducted; each study will be framed and conducted within the context of the countries discussed above.

4.3.2 Investigating Individual Perceptions

The main theme of the thesis is to discover how the human elements interact with an IDMS. As such, the individuals enrolled in IDMS form a key aspect of the investigation. Initial plans for this study involved the exploration of individuals' experiences through the various stages of the identity lifecycle, from enrolment to the actual usage and maintenance of the identity (for the identity lifecycle see Section 3.1.2.1). However, the cases under study made it impractical to capture an appropriate sample of individuals who had undergone the process.

Negotiations with the UK Identity and Passport service to follow up on enrolled individuals broke down, and the eventual decommissioning of the N-IDMS meant that it would be impossible. Similarly, the lead agency in India was unresponsive to any requests made.

Therefore, this study focused on individuals' perception of N-IDMS, aiming to discover the concerns that individuals have with regards to the collection, storage, and use of identity. Seeking to develop a holistic understanding of how individuals perceive an N-IDMS, the methodology used was chosen so as to capture rich descriptions of individuals' thoughts and reasoning when encountering identity systems.

4.3.2.1 Data collection – Focus Groups

Focus groups are an interview technique whereby a group of individuals are gathered to discuss a topic of interest. Compared to traditional interview techniques, focus groups provide a researcher with data that is more naturalistic (Silverman, 2004); dynamics of group interaction allows for spontaneous interactions and ideas to develop among participants, creating data that is socially constructed through synergistic effects where individuals respond to each others ideas. As (Krueger & Casey, 2000) state, the focus group method works because *"it taps into human tendencies. Attitudes and perceptions … are developed in part by interaction with other people"*.

Focus groups are particularly suited to extracting *"perceptions, feelings, and thinking of people about issues, products, services, or opportunities"* (Krueger & Casey, 2000), making them ideal in an attempt to uncover perceptions of N-IDMS. In order to build an understanding of the holistic experience that individuals have when encountering an IDMS, we need to provide individuals with an opportunity to openly discuss their thoughts.

One must also note the elusive nature of the concepts in question. Individuals rarely think about privacy and trust unless prompted by some kind of negative event or experience; i.e. unless presented with a situation that they can relate or empathise to, individuals only consider these aspects in passing. Therefore, it would be highly beneficial if subjects could bounce ideas of one another to flesh out ideas on how IDMS can affect themselves and society in general, thus providing interviewers with access to *"both actual and existentially meaningful experiences"* (Berg, 2001). This makes focus groups an ideal mode of inquiry for this aspect of the research.

Critiques against the use of focus group in the generation of theory, typically claim that it produces unreliable results. This stems from positivist quantitative realms that focus on test-retest reliability, which is argued to be impossible with focus groups, due to constant differences in the group construction. However, this is rebutted by Lunt & Livingstone (1996) who argue that the unit of analysis in focus groups is the thematic content of discussion, and *"not the properties of individuals composing the groups. Therefore, variation is not an error in the measurement of a property of an individual in the group, but rather the expression of variation in the discursive treatment of a topic for discussion"*.

The manner in which a focus group is conducted is steered by the features of the group(s) under study. These main *"characteristics relate to the ingredients of a focus group: (1) people who (2) possess certain characteristics and (3) provide qualitative data (4) in a focused discussion (5) to help understand the topic of interest"* (Krueger & Casey, 2000). These characteristics have implications for the study as listed below:

1. **People.** The number of people that are involved in each focus group. The literature in the area does not reach a particular consensus in this area. Recommendations spread from about 3 to 12 people (Kitzinger & Barbour, 1999). However, larger focus groups pose the danger of fragmentation, as individuals do not get the opportunity to speak. Small groups on the other hand suffer from fewer experiences and hence ideas (Krueger & Casey, 2000).
2. **Similar Characteristics.** Homogeneity of participants within focus groups is natural, as the participants are likely to consist of the people in whom you are interested. The level of similarity can vary from the vaguely general (e.g. a customer of a store) to highly detailed and specific (e.g. customers of certain age and gender who come from a specific area).
3. **Focused Discussion.** *"The topics of discussion in a focus group are carefully predetermined and sequenced, based on an analysis of the situation"* (Krueger & Casey, 2000). This means that the researcher should identify the areas of interest in the area of research. The questioning route, according to (Krueger & Casey, 2000), typically starts from general open ended questions, to stimulate early discussion and thought. Questions towards the end become more focused and specific**.**

The research here will make use of small highly structured focus groups. A small group size is deemed sufficient because of the complex nature of identity, privacy, and trust. A smaller focus group will allow participants to discuss and expand on their thoughts as needed. Furthermore, these groups are structured to elicit these elusive concepts, through the provision of scenarios that describe N-IDMS implementations (this is further elaborated later in the thesis in Section 6.2).

Although the focus groups were structured through the use of scenarios, measures were taken so as to prevent facilitator bias from influencing participants' answers. This was generally done by starting discussions with a broad open-ended question, which solicited participants' general thoughts on each particular scenario (David Morgan, 1996). The facilitator then guided each discussion based on the unique feedback received the particular focus group; i.e. the discussion moved from general to specific issues, revolving around issues that participants themselves have raised from the very beginning. This ensures that the moderator does not "*predetermine responses, and that they allow the opportunity for issues to arise which had not been anticipated*." (Lunt & Livingstone, 1996).

Given that we are looking at national scale IDMS implemented by governments, the population that we are interested in consists of the citizens of a particular country. It would be improbable to expect focus group participants to produce a representative sample of the population in a country. Practical limitations around time and funding make it impossible to conduct multiple large-scale focus groups that cover the diversity in the demographics of the population (i.e. age, education, work, income, etc.).

As such, the study used pragmatic sampling procedures; limiting participants to university students, which also helps to improve comparability of responses between groups. The demographics of the participants were selected to reflect the demographics of the user population in the case studies (Section 4.3.1); i.e. each focus group was made up of participants that were homogenous in terms of nationality (i.e. Bruneian focus groups, Indian focus groups, or British focus groups).

The disadvantage of only using university students in focus groups is that it is not a representative sample of the population. However, attempting to gather a representative sample of the population in 3 different countries was beyond the reach of this research project.

The British and Indian focus groups were conducted at the University College of London in the United Kingdom. Meanwhile, the Bruneian focus groups were conducted at the University of Brunei Darussalam in the country of Brunei; this was due to the fact that there were an insufficient number of Bruneian students studying within the United Kingdom; however, even while conducting it in Brunei, response rates to participation were very low. Ideally, the Indian focus groups would have been conducted at a local university in India, much like the Bruneian focus groups were in Brunei. However, attempts to contact local Indian universities for co-operation in arranging rooms for discussions and aid in the recruitment of participants were not entertained. Thus as a matter of practicality, it was necessary for the research to rely on Indian students at the University College of London.

A total of 43 participants took part in the focus groups. These were a mixture of postgraduate and undergraduate students studying a variety of subjects that are detailed in Table 5.

Table 5 Area of study for Focus Group participants

Subject	Number of Participants
Economics	3
Politics/Law	6
Engineering/Computing	10
Philosophy	1
Medicine	10
Science	8
Education	5

4.3.2.2 Data analysis – Grounded Theory

Grounded theory is an approach to develop theory that is grounded in data (Punch, 1998); grounded theory does not seek to test some preconceived theory, but instead seeks to start from an empty slate, and ends with a theory that emerges through a systematic collection and analysis of data (Corbin & Strauss, 1990). This approach to research requires a constant cycle of data collection and analysis until a point of theoretical saturation has been reached; i.e. no new theory is being generated.

Developing theory from data collected requires the breakdown of data to define what it is about, followed by its conceptualisation and reconstruction into theory (Charmaz, 2006). The process of grounded theory analysis consists of three different stages (Corbin & Strauss, 1990):

1. **Open coding** breaks data down into discrete events, situations, perceptions, etc. Instances and categories relating to the phenomena of interest are identified and grouped into concepts.
2. **Axial coding** develops relationships between categories, and the conditions that relate each category together. Reassembling the data that was broken-down in open coding.
3. **Selective coding** identifies the core category, i.e. the central phenomenon around which other categories revolve. A narrative is developed around this core category, forming the development of a storyline, which can further be developed into theory.

Grounded theory is suited to an exploration of events from individuals' perspectives. The aim of the individual study was to understand how individuals perceive systems, making grounded theory a suitable mode of analysis.

4.3.2.3 Exploring culture - Hofstede cultural value survey

The development of nationwide services impacts the population of countries as a whole, highlighting the role of national cultures in dictating the acceptance of an IDMS. By varying participants of each focus group on the basis on their nationalities, the data obtained can then be analysed and compared to that from the others, exploring the differences in the way that different national cultures react to similar systems.

The research conducted here will make use of Hofstede's (2001) cultural values survey as it is has the largest body of reproductions, and is continuously updated (Section 3.4.2). It is also the most popular model for measuring culture, and has been used in a variety of fields including that of privacy research.

Due to the small number of countries being looked at, a limitation is imposed on the application of cultural measures. *"Quantitative use demands data for a large number of countries, preferable ten or more; qualitative use is possible for any comparison of two or more cases"* (Hofstede, 2001). Furthermore, the qualitative application of the cultural values is better suited to the type of material and analysis produced from the focus group study.

4.3.3 Investigating Organisation Requirements

Organisations represent another component in IDMS research. The IDMS lies between the individuals and the organisations, thus requiring a balance among the needs of one group and the wants of the other. A successful implementation will need to take into account the impact that the organisation and its requirements will have on the system. The focus of the study is on the strategic vision of the organisation in relation to the N-IDMS.

4.3.3.1 Data collection – interviews and documentation

"Interviews may be defined simply as a conversation with a purpose" (Berg, 2001). The purpose, typically, refers to the collection of information about an item or phenomena of interest. It involves an interviewer *questioning* an identified interviewee about a particular subject on a one-to-one basis. There are several different methods that the questioning route can take.

Berg (2001) lists the three main types of interviews:

1. **Standardized interviews** have a formal structure, where interviewers strictly follow a set of pre-written questions.
2. **Unstandardized interviews** have no pre-defined questions, and interviewers adapt to each session.
3. **Semi-structured interviews** have some general questions to guide interviewers, while providing the freedom to adapt to each session, allowing for the examination of unexpected interesting points that may be raised in the session.

Semi-structured interviews themselves can be broken down into several different sub-types (Flick, 2002):

1. **Focused Interview.** This form of interviewing is designed to assess the impact of a stimulus on an individual. All interviewee's are presented with the same stimulus, enabling the researcher to analyse the differing subjective opinions.
2. **Semi-Standard Interviews.** Extensions of the semi-structured interviews, executed in two sessions. In the first session, the interviewee is asked to several different open-ended questions, which are then analysed. In the second session, the interviewee is asked to assess the analysis, and correct as needed.
3. **Problem-Centred Interview.** This interview style is focused on uncovering interviewee's view of a specific item of interest. This is done by asking specific questions, making use of interpretive statements, and confronting interviewee's with inconsistencies in their answers.
4. **Expert Interview.** Expert interviews differ from other interviews in that the interest lies with the role of the interviewee as a specialist in a field rather than the interviewee as an individual. This restricts the range of relevant information provided about the interviewee. These forms of interviews are useful when attempting to uncover professional considerations rather than personal accounts of events.
5. **Ethnographic Interviews.** These interviews resemble that of 'friendly conversation' rather than formal interviews, and typically occur spontaneously. Ethnographic interviews are used as support material for the observations that are typical of ethnographic studies.

The purpose of involving the organisation in this research is to account for the arguments that are put forward in support of an IDMS implementation. This research is not interested in the technical details, but rather in the reasoning behind the organisation's decisions. This thesis seeks to uncover the rationalisations and requirements that result in the design and implementation of an IDMS. To this end the research will make use of expert interviews.

The target population for the expert interviews are those individuals within the organisation that devise and influence the overall IDMS strategy in each of the case studies. Therefore, the experts need not be technical experts in the field, but those who are the leaders or key policy makers within the organisation. It is these individuals who will provide the research with insight into the government's intentions and concerns for the system and the impacts that it has on the eventual system design.

Furthermore, the organisation study also made use of official government documentation detailing the strategy and implementation of N-IDMS. This was especially true in situations in which government agencies were unwilling to come forward for interviews. Again, as with the choice of the expert interviews, the documentation collected and analysed were geared towards identifying the strategic motivations, and considerations that affected the implementation, design, and use of the IDMS in each of the three case studies.

4.3.3.2 Data analysis – Grounded Theory

The data obtained from the organisational study, was analysed using the grounded theory method (Section 5.3.2.2). The study is interested in identifying the process and planning considerations that go into the establishment and implementation of an N-IDMS; thus, grounded theory is a suitable medium with which to explore organisational concerns.

4.3.4 Exploring IDMS Design

Finally, apart from the individual and organisation, there is the IDMS itself. It is the core element, making it a critical part of this research. The investigation will revolve around the design of an N-IDMS and its impact on individuals' lives; design here is not used in the typical sense to refer to highly technical constructs, but rather to refer to the aspects of information flow and information type.

4.3.4.1 Data collection – Historiography

Historiography is an examination of elements in relation to some past event (Berg, 2001), the aim of which is to produce theoretical explanations for the subject of interest. This is differentiated from standard historical accounts in the sense that historiography is more descriptive and rich. It is not so much a nostalgic retelling of historical events as an expression of the nuances and meanings behind past events that have led to and influenced the present day situation. *"One cannot fully evaluate or appreciate advances made in knowledge, policy, science, or technology without some understanding of the circumstances within which these developments occurred"* (Berg, 2001).

Historical research can draw on a large source of materials from which researchers can distil and analyse past events. Materials of interests can range from government reports, newspaper editorials, folk songs, photos, artefacts, interviews, etc. These sources can be classified into two main categories (Berg, 2001):

1. **Primary sources** can be thought of as original accounts of events. A primary source is one that is produced as a direct outcome of the event in question; typically accounts created by those who have personally witnessed the events.
2. **Secondary sources** are second-hand accounts of the event in question. The producers of the material in question were not present at the time and place of the event of interest.

Typical applications of historiography attempt to establish a large body of primary source material for analysis. In fact, many consider the gathering of such material the core task of historical research. Berg (2001) does iterate and recognise the potential and importance of secondary sources in bringing together large bodies of material, and revealing details that are not otherwise apparent. The danger of using second-hand accounts is that some sources are actually written by authors who have little to no knowledge of the primary material (James Harvey Robinson, 1904). As a consequence, some secondary sources may in fact be four or six times removed from the original source; and typically the more a report is passed from mouth-to-mouth the less accurate or reliable it becomes.

History presents the system study with a vast resource of material and experience around the implementation of N-IDMS. In attempting to discover the impacts of practical IDMS design, it is important to acknowledge the context in which identity systems were required, and how this influenced the outcomes. Historiography provides an invaluable tool in approaching the material in question.

In contrast to the individual and organisation studies, the system study was not limited to the three cases identified previously (Brunei, India and UK; see Section 4.3.1). The system study draws on a richer base; it explores the historical development of identity that spans several different countries and timeframes. Furthermore, the investigation of well-known identity systems, of which the outcomes have been documented and reviewed by other experts, allows the study to focus on the exploration of the practical design aspects, and its impacts on everyday life.

4.3.5 Data Analysis - Thematic Coding

Thematic analysis is a method of investigating texts to deduce patterns that lie within the data (Marks & Yardley, 2004). In this form of analysis, a researcher goes through data gathered in one particular context, searching for and coding themes of interest, then comparing the themes to other similar contexts. Themes can either be developed deductively drawing from theoretical ideas that already exist, or inductive in nature, being developed from the data itself (Marks & Yardley, 2004).

Thematic coding requires a priori identification of various items under study (Flick, 2002); sampling of material is chosen to increase the comparability to other contexts. Additionally, the unit of analysis should be defined beforehand. Coding of the material is guided by the research question. Codes are developed for each case, compared and cross checked with one another and then refined by splitting, splicing, and linking the codes (Marks & Yardley, 2004).

Thematic analysis was used to investigate the practical design of IDMS, and its effects. Several different implementations of N-IDMS were chosen across various timeframes and purposes, allowing for comparisons that stretched various boundaries, strengthening the themes that were developed. Given the depth of each system, the unit of analysis chosen was that of the case level. The material on each N-IDMS was brought together to form a complete narrative of the situation, which was then analysed, picking out system attributes that influenced outcomes and interactions.

4.4 Triangulation

Finally, this thesis makes use of triangulation as a form of verification, and a method to bring the three different studies together. Triangulation is a method that researchers make use of to gain a robust and through understanding of the research problem. The term has been borrowed from the land surveying field, in which it is defined as a *"method of location of a point from two others of known distance apart"* (Flick, 2007). From a methodological research standpoint, triangulation involves the use of multiple perspectives to study the issue of interest. As one of the earliest proponents of triangulation in qualitative research, Flick (2007) states that the advantage of triangulation is that it helps to reduce personal bias that arises from single method or single investigator research. Triangulation acts as a form of validity checking, as theory generated comes from a variety of sources.

There are four different techniques to perform triangulation (Flick, 2007):

1. **Data Triangulation** is the collection and analysis of different sources of data. This can be achieved by studying instances of the same phenomenon in different settings, for example different points of time, different people or different locations.
2. **Investigator Triangulation** is the use of multiple researchers to minimise investigator bias of a single person. It involves a systematic comparison of various observations and the different influences of each researcher.
3. **Theory Triangulation** Denzin & Lincoln (1998) describe this as *"approaching the data with multiple perspectives and hypotheses in mind"*. When different theories exist, a researcher can then view the problem from different standpoints, finding the one that fits best.
4. **Method Triangulation** involves the use of multiple methods that are carefully chosen to maximise the validity of efforts. The research methods employed should play off each other's strengths and weaknesses.

While the use of triangulation does not pose a problem to those who approach research from a pragmatic paradigm, certain critics, especially interpretivists, have voiced their reservations; interpretivists argue that any discoveries made using one particular method or data source do not capture the *same* phenomenon as those made with another. However, in spite of this, critics still find value in triangulation, such that when combined, different traditions will produce a fuller picture of the phenomenon. It provides the research with range and depth that would otherwise not be captured (Flick, 2007).

The research conducted here will make use of two forms of triangulation; data and method triangulation. The use of multiple data sources, and methods to investigate them, can be observed from the three different approaches to N-IDMS, i.e. the system perspective, the individual perspective and the organisational perspective. This approach will provide the research with the depth that is required to fully understand the phenomenon in question.

The use of triangulation is also useful in bringing together the outcomes from each of the study into a single coherent framework. Construction requires the identification of overlaps and relationships between each strand of research, enabling the construction of one *complete* narrative that describes the entire situation. This process also lends validity to the overall findings, as each study supports and validates the results of the other.

4.5 Chapter Summary

The aim of this research is to take a human-centred approach to IDMS. It seeks to explore the relationship that human factors have with such systems. With this in mind, the methodology used should reflect the goals that have been set out. Considering the complex socio-technical interactions of such systems, the research requires the use of various data sources and methods to suit the different contexts under investigation.

The investigation is broken down into three main areas of exploration. Firstly, a system study is carried out. Using historiography as a main tool for data collection, it is supported by the use of thematic analysis to uncover how the design of an IDMS affects the lives of individuals.

The other two areas of investigation tackle the issue from an individual and organisational perspective. These studies will be guided by a case study methodology based on three different countries; Brunei, India, and UK. The individual study will make use of focus groups to explore how individuals assess IDMS. The influence of culture on individuals will be approached using Hofstede's cultural values to identify differences between countries.

Meanwhile, the organisation study will be investigated through material collected from official documentations and interviews. Both areas of investigation will make use of grounded theory to develop explanations directly from the data.

Finally, the research will make use of triangulation to bring all the data together into a single coherent framework that provides a holistic view of human-centred IDMS. This also acts as a form of validation, as theory generated from various sources is checked against, and reinforces, that from others.

Chapter 5: System Study – Lived Experience of Identity

This chapter presents a framework that outlines how the design of an IDMS can affect the *lived experience*. **For an alternate reading, please refer to Appendix IX**.

The literature review has revealed that privacy research is largely tackled within an informational privacy perspective, meaning that emphasis is placed on confidentiality, treating individuals and their identities as static functional objects (Section 3.2). Recent debates call for a focus on the larger issues that surround identity, focusing on the consequences of collecting, storing, and using personal information.

Focusing on the outcomes of identity, the framework here identifies a set of design properties that impact individuals' everyday lives. These properties were identified through an analysis of public response to 15 past and present national identity systems (Section 5.1.1). They capture the practical design aspects of an identity system, from *structural properties* that affect the flow of information – *Control Points, Subject Engagement, Identity Exposure, Population Coverage* – to the *metrical properties* that considers how information is used and perceived – *Expert Interpretation, Population Comprehension, Information Accuracy, Information Stability, Subject Coupling, Information Polymorphism* (Section 5.2.1 and 5.2.3).

Any identity system can be described in terms of these fundamental properties. Practitioners and researchers would make use of this framework by analysing an identity system in terms of the various properties, and the impacts of these properties on the *lived experience* (Section 5.3).

5.1 System Research

As outlined in Chapter 4 this thesis seeks to address the research question by tackling the problem from three different perspectives; i.e. the system, individual, and organisation. This chapter presents the system study that investigates the effects of an IDMS individuals lives.

The type of information and the way in which it is used can have an impact on the outcomes for an individual (Section 3.2). However, traditional approaches to identity abstract the IDMS away from the specific consequences that it has on individuals' lives, and the various coping strategies that might be adopted. Experts talk about data minimisation or ease of use, but what does it mean to an individual? How does it affect an individual's relationship with the organisation and society? The current frameworks have been useful for the development of better systems, but in applying these principles we lose sight of the entire context of implementation; i.e. the *identity ecosystem* that recognises the relationships that exist between the individual, system, and society.

The concept of the *lived experience* increases the scope of human-centred design beyond traditional usability concepts, which are *"directed more toward functional accounts of computers and human activities* (McCarthy & Wright, 2004). Designing for the lived experience requires an understanding of *"the relationship between people and technology in terms of felt life and the felt or emotional quality of action and interaction"* (McCarthy & Wright, 2004).

Inglesent and Sasse (2001) go on to elaborate that "*the lived experience emphasizes the ways in which difficulties at the interface can lead to serious disruptions away from the interface in the lives of users*". As such in this thesis, the lived experience of identity is defined as the effect of the collection, storage, and use of identity information on all areas on individuals' everyday lives, freedoms, and interactions. The benefit of such a definition over traditional views of information privacy and trust (Section 3.2.3), is that it broadens the scope of identity research towards the overall implications of identity. In so doing, identity research is focused on the meaning of identity for the individual.

Practitioners and researchers require a way of analysing the lived experience that results from participating in an identity ecosystem. They require a framework that will allow them to assess how the designs of an identity system might influence an individual's everyday lives, and thus their roles in society.

5.1.1 Methodology

In order to distil the impacts of an IDMS design on the lived experience, the study analysed a total of 14 different past and present N-IDMSs, for which the outcomes are already known. The scope of that review was limited to N-IDMSs implemented in the Western world, largely focusing on a timeframe extending from the medieval periods to the present day; according to Torpey (2000), these countries have been leading the development and adoption of modern identity systems.

Historiography (Section 5.3.4.1) was used in the information collection phase, with the aim of developing a brief narrative that describes the overall development of each N-IDMS, and the reactions of individuals to the system; these narratives can be found in the form of a literature review in Chapter 2 and is summarised in Table 6.

The development of this narrative relied on secondary sources; the reliance on material that provided second-hand accounts was necessary as the review spanned various timeframes and countries, resulting in the inaccessibility of certain material, as well as language barriers posed by original material. The accounts that were used were chosen for their depth, accuracy and recognition in their field. To account for the dangers of using secondary accounts (Section 4.3.4.1), where possible, the research relied on secondary sources that includes or references directly from original documentation. Furthermore, secondary accounts used were chosen based on the depth of analysis, as well as recognition in the field.

The data collected was analysed using thematic coding to identify similarities across each N-IDMS narrative (Section 4.3.5); the focus of the analysis was on identifying the practical design aspects of an IDMS that had an impact on the outcomes of each implementation under review. Each N-IDMS was treated as a separate case, where features of each system that led to the various outcomes were coded. The analysis took place in three main phases:

1. **Reviewing accounts of each implementation, determining the degree of adoption, and the various reactions towards the system; did individuals sign up to a voluntary system? Did they attempt to evade non-voluntary systems? Did they change their habits as a result of being part of the system?**

2. **Discover the arguments that lead individuals to react in the manner identified; how did they feel about the system?**
3. **Code the basic features, i.e. the design properties of the system that brought about the identified reactions of individuals.**

Table 6 List of N-IDMSs analysed, along with the country of origin and overall purpose.

System	Country	Purpose
Poor Laws and Badges	United Kingdom	To provide members of organisations proof of association
Criminal 'Wanted' Lists	Medieval Europe	To provide for accurate identification of individuals especially criminals
Internal Passports	Russia	To track movement of locals in the country
Passports	Netherlands	To prevent or monitor the entry of dangerous foreign radicals into the country
French Nomad Law	France	Identification and monitoring of unwanted members of the population
National ID Cards	United Kingdom Germany	To provide unique identities to individuals allowing easy identification of the entire population
Bertillonage	France	To identify recidivists enabling enforcement of severe punishment
Dactyloscopy	Argentina	To identify recidivists enabling enforcement of severe punishment
US Visit Programme	United States	To identify criminals and terrorists entering or leaving the country
UAE Iris Scan	United Arab Emirates	To accurately identify known individuals against captured Iris scans (e.g. criminals)
Criminal DNA Database	United Kingdom	To accurately identify individuals against DNA samples
Contact Point	United Kingdom	To identify children in need of protection services before serious harm is caused
PKI and Digital Signatures	Austria	To provide individuals access to services in a virtual environment

5.2 Analysis

The results of the coding process revealed that the practical design properties of an N-IDMS that influences outcomes can be grouped into two main categories, each of which are made up of several different properties (**Table 7**):

1. **Structural properties** that capture the flow and relationship of an individual's information within the identity ecosystem created.
2. **Metrical properties** that capture the qualities that are affected by the type and amount of information that is being collected and used in the identity system.

Table 7 A description of the system design properties that account for the lived experience of identity.

Structural Properties	Metrical Properties
1. Number of Control Points express the situations in which an individual's identity is required in order to proceed with a particular function	**1. Population Comprehension** is the general level of understanding that the general population has regarding the techniques and technologies used for identification
2. Subject Engagement captures whether an individual is an active or passive participant in the use of the identity.	**2. Expert Interpretation** captures the amount of human activity required to collect and use identity information
3. Identity Exposure refers to the degree of control that individuals have over the presentation of their identity to other individuals or relying parties that have no right to that identity.	**3. Information Accuracy** is the property that defines the reliability of the information that is collected, stored and used in the identity system.
4. Population Coverage describes the number of individuals that are registered in and interact with the system, in relation to the size of the total population	**4. Information Stability** refers to the rate with which the information stored in an identity system changes over time
	5. Subject Coupling expresses the degree of representativeness between the captured identity and the relevant partial identity
	6. Information Variability expresses the ease with which the identity information may be used for a different purpose

Analysis was done until theoretical saturation was reached, within the set of cases that made up the study. This would imply that there might be other design properties that may be revealed by analysing other identity systems. For example, an expert evaluating the findings of this study has put forward the property "system fuzziness" in reference to federated identity systems (Section 9.2.3.1). However, with that said, the properties that have been uncovered in this research have been derived from a varied set of implementations, and will later in this chapter, be shown to be applicable in other contexts such as Social Networking (Section 5.3.2), and Personalized Advertising (Section 5.3.3). As such, the properties here are the key design properties that are applicable to any form of IDMS.

In order to aid clarity and understanding, the following sections will introduce the design properties, and their impact on the lived experience, within the context of the various N-IDMS implementations; this is done through a systematic review of the technologies that enable the presentation and use of identity (Section 5.2.1), as well as the type of information that makes up the identity (Section 5.2.3).

5.2.1 Analysis of Structural Mechanisms and Their Properties

The structure of an IDMS captures the flow of information within the identity ecosystem; it is concerned with the mechanisms that enable the use and consumption of an individual's identity. It defines how individuals and societies interact with, and are shaped by the IDMS.

Drawing from the review of the past and present N-IDMS implementations, a breakdown of various structural mechanisms is provided, detailing its operation, and its impact on the lived experience; in this process the practical design properties of the structural components are highlighted.

5.2.1.1 Reproducible tokens

Reproducible tokens are identity documents that emphasise the use of symbols and emblems as a means of recognition. Making use of common insignias and symbols, these tokens were suited for use in identifying group membership, where rights to perform certain acts were endorsed by organisations onto their members (Groebner, 2001).

With the **Poor Laws**, tokens were distributed to beggars in the forms of badges that allowed them to request for alms (Section 2.2.1.2). However, few beggars actually came forward and instead resorted to a life of crime. Unfortunately, since the badges were related to that of a perceived lower class, they eventually came to be seen as a mark indignity (Hindle, 2004). As badges were to be worn at all times (*high Number of Control Points*), and were visible to everyone (*high Identity Exposure*), beggars refused to cooperate (*high Subject Engagement*). In addition, the highly targeted nature of the system (*low Population Coverage*) meant that individuals lost control over their dignity in within society.

Turning attention to the **Nazi branding of the Jews** shows the effect more sinister applications of tokens have on the lived experience (Section 2.2.2.1). Seeking to make outcasts of the Jews, the government made effective use of tokens to target individuals' social construction; the identification system became a powerful weapon in the government's arsenal (Fussell, 2004).

> *"Identification had a paralyzing effect on its victims. The system induced the Jews [low Population Coverage] to be even more docile, more responsive to command than before. The wearer of the star was exposed [high Identity Exposure]; he thought that all eyes were fixed upon him. It was as though the whole population had become a police force, watching him and guarding his actions [high Number of Control Points]. No Jew, under those conditions could resist, escape or hide without first riding himself of the conspicuous tag, the revelling middle name, the tell-tale ration card, passport and identification papers [high Subject Engagement]" (Hindle, 2004).*

With the development of stigma around group membership, the Jewish population lost a sense of control over their lives, creating a negative lived experience. Additionally, the badges here were paralyzing for an individual, as society merely lumped them into groups.

5.2.2 Personal Documents

In contrast to reproducible tokens, personal documents are identifying mechanisms that focus on distinguishing unique individuals from a group rather than to assign them to one. After being issued unique documents, it is up to individuals to present and make use of the mechanism as needed. As such, the system is best operated for situations when an administration wishes to control access to certain privileges based on varying individual attributes.

The **Russian Internal Passports** are form of personal documentation that was introduced to restrict movement of the local population within the country (Section 2.2.3.1). However, the extreme demands of the system fuelled evasion attempts. Based on (Matthews, 1993) analysis of the passport system showed that the lack of compliance may be due to the large number of bureaucratic loops that an individual had to go through (*high Subject Engagement*), as well as the large number of checkpoints where the identity documents were to be presented (*high Number of Control Points)*; individuals lost their believed right to free movement, and thus rejected the system with its large number of controls.

The introduction of the **Dutch Passports** in the early 19th century was also designed to control movement (Section 2.2.3.2). However, compared to the Russian Internal Passports, the focus was on movement into the country at its borders (*low Number of Control Points*), making it a much less restrictive system, and less of a burden to adhere to. Documents remained in circulation even after the passport requirements for travel were removed; this was largely driven by the benefits of security against harassment by law officials in foreign lands (Lucassen, 2001).

The **French 1912 Nomad Law's** provide greater insights into the effect of the structural properties on the lived experience (Section 2.2.3.3). The introduction of the law and passes was met with mixed success. The gypsy population (*low Population Coverage*) were required to present the passes (*high Subject Engagement*) upon entry and exit of every commune (*high Number of Control Points*). The result was a highly discriminatory system, placing difficult burdens on a specific set of the population; as a result, some of the gypsy population gave up their way of life to free themselves of the hardship (Kaluszynski, 2001).

Finally, the demise of the **British World War I identity cards** also highlights the impact of the number of checkpoints (Section 2.2.2.2). The implementation of the system was based on an act that enabled the creation of a National Register during the period of war, and was thus abandoned shortly after the war ended. Additionally, there is also evidence of public intolerance to the *prussianizing* aspect of the system, with its endless reporting and interference (*high number of Control Points* and *high Subject Engagement*) was the downfall of the system. "*Public anxiety over the state interference which maintenance of the register implied*" meant that many individuals failed to update their information such as change in address, leading to an inaccurate identity system.

Similarly, the **British World War II identity cards** were abolished after an individual refused to produce his identity document (*high Subject Engagement*) when randomly stopped by police officers (*high Control Points*); the judge presiding over the case claimed that *"to demand registration cards of all and sundry… is wholly unreasonable"* (Agar, 2005).

5.2.2.1 Database/Register

In the basic meaning of the term, databases are a centralised collection of records that are gathered for a specific purpose. Databases are a key component of criminal identification systems that enables law enforcement to record, identify, and track criminals.

The privacy concerns in the **UK DNA Database** can be partly attributed to the high degree of centralisation in the system design (Section 2.3.4.1). Whenever a crime is committed, law enforcement agencies may match samples obtained from crime scenes against the whole DNA database (*high Number of Control Points*), without individuals' knowledge (*low Subject Engagement*). The constant access of individuals' information, coupled with their passivity in the interaction creates feelings of uneasiness, thus fuelling privacy concerns.

Furthermore, traditional criminal IDMS, such as **Bertillonage** and **Dactyloscopy**, have historically been targeted towards convicted criminals. Meanwhile, the UK DNA database increases this scope to cover all suspects, including those whom are not convicted of any crime. However, overall it is still a discriminatory system, covering only seven per cent of the total UK population (*low Population Coverage*); as a result, innocent suspects are treated differently from the rest of the population, this further creates feelings of uneasiness among the population, as innocent individuals may be treated like criminals.

5.2.3 Analysis of Identity Metrics and Their Properties

While the system structure defines how identity is applied, the identity metric deals with the kind of information that represents identity; it is concerned with the type of information that is captured, presented and used in various identity requiring situations.

5.2.3.1 Biographical information

The use of biographical information is a common way to construct an individual's identity. It can revolve around something as simple as a name, to a whole collection of life experiences. The relevant identity information in any context is defined by the role that an individual adopts in that context.

During Medieval times individuals, **wanted lists** of criminals typically only described criminals by the attire as opposed to any physical attributes. At the time clothes were expensive, and could be rarely changed. However, clothes eventually became cheaper and more accessible, and thus became an unreliable form of identification. The dynamic nature of the information (*low Information Stability*) used to represent identity meant that criminals could easily evade identification by simply changing their attire.

The lived experience of the **French Nomad Law** was not only affected by the structural properties outlined earlier (Section 6.2.2), but may have been further influenced by the chosen identity metrics. The scheme was effective because the identity was constructed so as to closely represent the targeted individuals' nomadic lifestyle (*high Subject Coupling*), which happened to be highly dynamic in nature (*low Information Stability*). Thus, when individuals chose to abandon the gypsy lifestyle, they were freed from the burden of having to maintain a constantly changing identity.

The purpose of the **Contactpoint Database** was to quickly identify children at risk of abuse by sharing information across different government services. However, critics claimed that it would not work, as it wasn't the lack of information that prevented detection of child abuse, but the way in which carers interpret the information; identifying child abuse is a highly subjective process (*high Expert Analysis*). Concerns about e-discrimination and self-fulfilling prophecies were also raised when law enforcement wanted to use the Contactpoint database to identify future criminals. Arguments centred on the fact that irresponsible behaviour is not a good indicator of future criminality (*low Subject Coupling*). Furthermore, children are constantly growing and developing new behaviours, implying that the information may be quickly changing (*low Information Stability*), and therefore may lead authorities to make decisions based on out-dated information.

5.2.3.2 Biometric data

Biometric identification is the use of physiological characteristics to recognise individuals. It is based on the principle that certain biological attributes are unique, and are hence suited for identification of individuals. This section covers the biometric technologies that were implemented in the IDMSs that formed part of the review.

5.2.3.2.1 Anthropometry

Despite being a step forward from conventional criminal IDMS at the time, the use of anthropometry in the **Bertillonage** system possessed certain limitations (Kaluszynski, 2001). For example, it was not applicable for use in the identification of women, due to pathological disturbances (e.g. pregnancy), or children, who were still growing (Cole, 2001; Fosdick, 1915). This produced constantly changing measurements (*low Information Stability*), which allowed such individuals to evade identification as recidivists. Furthermore, despite the extensive training provided, measurements still required a certain amount of interpretation and subjectivity (*high Expert Analysis*). Coupled with the ability of the individual to force erroneous measurements through subtle movements (*low Information Accuracy)* meant that the performance of the Bertillon system was negatively affected.

Finally, perceived human rights violations attached to the Bertillon system also hampered its success in Argentina. The public viewed the anthropometry procedures as being intrusive and *"damaging to the soul"* (Ruggiero, 2001). This misconception of the identity metric (*low Population Comprehension*) led to the destruction of anthropometric records of criminals who have completed their sentence thus preserving their honour and dignity (Ruggiero, 2001), making the system useless for identifying recidivists.

5.2.3.2.2 Dactyloscopy

Dactyloscopy had two main advantages over the Bertillon system for identifying criminals. Firstly, the use of rolled fingerprints provided a form of *mechanical objectivity* in the capturing of identity, thus creating more accurate records (*high Information Accuracy)*. Secondly, fingerprints could be used in forensic investigations.

However, caution should be taken in charging criminals based only on fingerprint evidence. For example, an early application of dactyloscopy to a murder investigation in 1898, saw a judge deem that the fingerprint evidence was only sufficient to prove trespassing and not murder (*low Subject Coupling*) (Cole, 2001). From this, we can deduce that the level of representativeness in the forensic use of fingerprints was already called into question from its early applications; finding a fingerprint at a crime scene does not equate to proof of guilt.

Yet, in its practice today, fingerprint identification in criminal cases carry a lot of authority, of which is rarely questioned (Cole, 2001). An exemplar is the **McKie case**, in which Shirley McKie was arrested, charged, and prosecuted based only on fingerprint evidence allegedly found at the crime scene (*low Subject Coupling*). In an ordeal that last 9 years to resolve and gain compensation, authorities did not concede any error in the positive identification by their fingerprint experts, even in the face of other expert testimonies who claimed otherwise (*high Expert Analysis*). Although a public inquiry ruled out any collusions, identity systems that do not tackle this issue are a danger to public justice and freedoms, where individuals may be charged on little evidence that is put forward by unregulated 'trusted' experts.

Meanwhile, also making use of fingerprints, the increased scope of the **US Visit** scheme from visa authentication towards security and terrorism presented some problems. In matching fingerprints against criminal databases, individuals who produced a 'positive identification' were automatically treated as dangerous without further consideration, including aircrew members who had already successfully passed through previous background checks (*low Subject Coupling)*. The situation was exacerbated by the inaccurate fingerprints available on databases, and the general low performance of a one-to-many fingerprint search (*low Information Accuracy*); to date, the system has only caught one terror related suspect.

The improper use of fingerprints for counter-terrorism is further elaborated by the **Brian Mayfield case**. Mayfield was placed on police custody for two weeks based on FBI claims that fingerprints found on Madrid bombing site were an *"absolutely incontrovertible match"* (*low Subject Coupling*) (Isikoff & Pape, 2004; Murr, 2004), based on erroneous applications of the fingerprint identification methodology by their experts (*high Expert Analysis*).

5.2.3.2.3 DNA

As with fingerprints, DNA data lends itself to forensic investigations. However, as with fingerprints, forensic DNA investigations present similar problems of infallibility of expert identifications. In the **UK DNA Database** scheme, the **Easton case** illustrates a situation where Mr Easton was a prime suspect in a burglary case based on DNA evidence; this despite his Parkinson's condition that indicated he could not have committed the crime (*low Subject Coupling*).

The **Madeleine McCann case** highlights issues about public understanding of identity systems. When traces of DNA were found in the car hired by her parents, many people falsely perceived this as a sign of guilt, likely due to the lack of comprehension around the process and probabilities – "*one in trillions"* (Graham, 2007) – of DNA typing (*low Population Comprehension*). Not only were the McCanns forced to deal with the trauma of losing their daughter and questioning by the police, but they were also forced to deal with the negative reaction of the public in light of their perception of the DNA evidence; early public support for the McCanns quickly turned to accusation and attacks against them.

The deterministic nature of DNA identification is further exacerbated by the subjective matching decisions that are made (*high Expert Analysis)*, against contaminated or degraded crime scene samples (*low Information Accuracy*). The 1993 **Timothy Durham case** in the United States serves to illustrate this problem; despite having a strong alibi, Durham was found guilty of raping an 11-year-old girl, largely on the basis of DNA evidence (Thompson et al., 2003). Durham was set free in 1996, after it was shown that there was an error that *"arose from misinterpretation",* due to the failed separation of the contamination between the male and female DNA during extraction of the semen stain (Thompson et al., 2003).

Apart from the misunderstandings of DNA identification process, the nature of the data itself has raised privacy concerns. DNA can not only be used for individual identification, but also for a number of other purposes such as identifying racial heritage and familial linkages, or the likelihood of developing certain illnesses (*high Information Variability*). The use of the **UK DNA database** in familial searching, constant requests for paternity tests, and its recent call for use as a medical database are prime examples of how DNA can be easily used for other purposes. The possible function creep and unpredictability around the use of the identity is seen as a threat to privacy that can negatively affect individuals.

5.2.3.2.4 Iris

Iris recognition is seen as one of the most stable and accurate forms of biometric identification, however lacks forensic applications (although the increasing use and improvement of CCTV technology and iris recognition algorithms may make it a reality in the future). As a result, identity systems using iris recognition tend to produce good results.

The **UAE Iris system,** implemented at the country's borders to prevent banned individuals from coming into the country, has been a big success. Everyone passing through these borders is exposed to the system. Iris captures are matched against a database of high quality iris images (*high Information Accuracy*) of banned individuals, ensuring that a match is likely to correlate well with a known individual (*high Subject Coupling*); as opposed to inaccurate crime scene samples used in fingerprint systems seen previously (Section 6.2.3.2.2). To date, it is claimed that the system has not produced a false match despite processing 2.7 billion comparisons per day, while preventing the re-entry of 9,500 banned individuals (Kabatoff & Daugman, 2008).

5.2.3.3 Digital Signatures

A digital signature is a cryptographic based technique to simulate the function of a real world signature in a digital environment (not to be confused with digital signature recognition which is a biometric that has seen limited implementation). Despite the promise of digital signatures, uptake among the public tends to be rather low due to its complexity.

The review of the **Austrian Citizen Card** and **Belgian** eID scheme show incredibly limited adoption of digital signatures, which has been attributed to a lack of opportunities to actually make use of the digital signatures (*low Number of Control Points*) and the lack of understanding on how it works (*low Population Comprehension*). Similarly, in a study of merchants trading through Amazon (Garfinkel, Margrave, Schiller, Nordlander, & Miller, 2005) found that only 54% of those who received digital signatures know how they worked. Furthermore, 59% per cent of merchants thought it was important to use encrypted and signed mail, yet 59% also admitted to not knowing whether their email client supported it.

5.3 Towards the Lived Experience

In introducing the properties above, this thesis has illustrated its use in understanding the lived experience. In certain configurations, such as an identity system with a high number of *Control Points*, the system might be perceived as being too cumbersome and oppressive, and thus might be met with resistance. A system that needs to be up-to-date, but makes use of a metric that has a low *Information Stability,* may be seen as a burden upon individuals, who continuously have to report changes in their personal information.

However, reactions against identity systems are rarely caused by any single property; it is the combination of these various properties, and their interactions, which determine the lived experience. One can then construct the possible narratives and potential outcomes based on the various contextual elements and social norms. Consider a system with *low Population Coverage*, *high Subject Engagement*, and a *high Number of Control Points*. The resulting system is highly targeted towards certain criteria, while the majority of the population acting in that particular context would not be troubled. Additionally, as individuals play an active role at a large number of *Control Points*, some might decide that the burden of the system is unbearable. As such, in cases where it is possible to do so (e.g. identification systems based on religion), a number of individuals might avoid the identity system altogether by abandoning their current identity, and constructing a new one, as was the case with the French Nomad Laws; being enrolled in such an IDMS is a form of punishment or a means of controlling behaviour and forcing change.

For the DNA database, most of the properties introduced here are relevant to interpreting the public reactions towards the system (Table 7). The initial set of privacy concerns stem from the constant access of the identity (*high Number of Control Points*) of which the individual is unaware (*low Subject Engagement*). This is further amplified by the possibility that the identity information can be easily reused for other purposes in completely different contexts (*high Information Variability*), again potentially without the individual being aware of this.

Issues of fairness and freedom also come into play when considering the highly targeted nature of the DNA database (*low Population Coverage*), especially in light for the lack of control that an individual has over the presentation of the identity to the rest of society (*high Identity Exposure*). Furthermore, the lack of control is substantially worsened by the incomplete yet deterministic nature of such identification (*low Subject Coupling*) that is based on subjective assessment (*high Expert Analysis*) of potentially inaccurate information due to contamination and degradation (*low Information Accuracy*).

Based on this narrative for the DNA database, it is not surprising that the system is surrounded by privacy concerns and controversy. These concerns are given strength, perhaps counter-intuitively, by the broadening of the *Population Coverage*, as it includes not only convicted criminals but suspects as well. This can perhaps be explained by the fact that it is still a highly targeted system, just broader in scope. Additionally, from the point of view of innocent suspects, they do not believe themselves to belong on the database at all, meaning the partial identity created goes against the relationship between the individual and the state, thus further driving down the level of *Subject Coupling*.

The combination of all these properties creates a very negative lived experience that influences society's interactions with the individual. The risk of false accusations, based on minimal evidence, that people do not understand, put forward by 'infallible' experts, based on potentially erroneous data, creates problematic situations that individuals are not able to overcome or fight against. Such a scenario would fundamentally change the relationship of the individual to society. The public will vilify these individuals, while interactions with organisations will be mediated by these suspicions thus creating self-fulfilling prophecies.

Table 8 A summary of the system analysed in this study, their design properties, and impacts on the lived experience

System	*Structural Properties*				*Metrical Properties*					
	Control Points	*Subject Engagement*	*Identity Exposure*	*Population Coverage*	*Subject Coupling*	*Population Comprehension*	*Expert Interpretation*	*Data Accuracy*	*Data Stability*	*Information Variability*
Poor Law Badges	*High*	*High*	*High*	*Low*	*Low*	*High*	*Low*	*Medium*	*Low*	*High*
	Few people came forward to request for an identity. *Beggars were required to prove that they could not get work. They were required to wear badges at all times in order to prove that they have the right to request for alms. A small number of individuals had to constantly wear badges on their arms, which were clearly visible to everyone else. This shamed individuals, making them unwilling to come forward. Furthermore, the information was also to determine parenting ability, a purpose that differs from the original.*									
Criminal Wanted Lists	*Low*	*High*	*High*	*Low*	*High*	*High*	*Low*	*Low*	*Low*	*Low*
	High rates of evasion. *The system is based on a simple set of physical descriptions that had a focus on the attire of individuals. This data was not very accurate and involved a high degree of subjective decisions as to a match. Furthermore the individual can easily change his physical appearance by donning disguises or new attire.*									
Russian Internal Passports	*High*	*High*	*Low*	*High*	*Low*	*High*	*Low*	*Low*	*High*	*Low*
	Large number of evasion attempts and manhunts were frequently launched. *The identities created tied individuals to a piece of land where they were required to work. This identity was rejected by individuals who did not agree with the relationship and attempted to flee from the state.*									

System	*Structural Properties*				*Metrical Properties*					
	Control Points	*Subject Engagement*	*Identity Exposure*	*Population Coverage*	*Subject Coupling*	*Population Comprehension*	*Expert Interpretation*	*Data Accuracy*	*Data Stability*	*Information Variability*
French 1912 Law	*High*	*High*	*Medium*	*Low*	*Low*	*High*	*Low*	*Medium*	*Low*	*High*
	Part of the targeted population (Romani) abandoned their way of life and assumed new identities. *The system was a burden on individuals, constantly showing their identities whenever they moved. Being a highly targeted system, an individual can avoid the system by "changing" his/her identity.*									
French Bertillonage	*Low*	*High*	*Low*	*Low*	*High*	*Medium*	*High*	*Low*	*Low*	*Low*
	Reliability and effectiveness of recidivists was called into question. *The identification process was highly subjective using inaccurate information, resulting in inconsistent identifications. As individuals were involved in the identification process, they could alter their dimensions by not fully co-operating, e.g. not standing straight, etc. Furthermore, it was ineffective at identifying young individuals as they were still growing.* *In Argentina, system was rejected on grounds that the measurements insulted their honour. It can be argued that they either did not understand the process or they felt that it was a misrepresentation of their identity.*									

System	*Structural Properties*				*Metrical Properties*					
	Control Points	*Subject Engagement*	*Identity Exposure*	*Population Coverage*	*Subject Coupling*	*Population Comprehension*	*Expert Interpretation*	*Data Accuracy*	*Data Stability*	*Information Variability*
Argentina Dactyloscopy	*Low*	*Low*	*Medium*	*Low*	*Medium*	*Low*	*High*	*Medium*	*High*	*Low*
	Dactyloscopy has become a de facto standard in criminal investigations. *Fingerprints collected did not change over time and was more accurate than body measurements or descriptions. It gave the identification of criminals a form of "mechanical objectivity" in that the fingerprints were captured using objective approach.* ***Issues of false accusations have recently been called into question.*** *Dactyloscopy still requires subjective decisions to decide if there is a match. Crime scene fingerprints are not accurate representations of fingerprints, further raising the error rate. People are not aware of the entire fingerprint identification process and therefore individuals lose the ability to resist such accusations.*									
WW I and II UK Identity Cards	*High*	*High*	*Low*	*High*	*Low*	*High*	*Low*	*Medium*	*Low*	*High*
	Individual information was out of date. *The information collected included attributes such as address which were open to change. The high variability in the information collected and stored, required the co-operation of individuals to update their records as needed. The public however proved unwilling to assist them in these procedures, especially since the cards did not provide any benefits after war time (after its use in food rationing). It is perceived as the needless prussianizing of institutions.* ***Resistance to carrying and showing ID Cards.*** *The needs for identity cards represent a clash in the culture for the public. The identity created by such a system goes against the relationship that exists between the state and its people. Therefore, the identity instantiation did not match well to the individuals' perception of the situation. This led to resistance towards hosing ID cards, as in the case of Wilcock, which was brought to court and gained a lot of public support and negative media publicity against the ID cards.*									

System	*Structural Properties*				*Metrical Properties*					
	Control Points	*Subject Engagement*	*Identity Exposure*	*Population Coverage*	*Subject Coupling*	*Population Comprehension*	*Expert Interpretation*	*Data Accuracy*	*Data Stability*	*Information Variability*
WW II Nazi Jewish Identity System	*High*	*High*	*High*	*Low*	*Low*	*High*	*Low*	*High*	*High*	*High*
	Paralysis of the Jewish Population. *The identity system created was highly targeted to the Jewish population. It started off as an identity document with clearly stated markings, indicating the individual was a Jew. This eventually led to the use of symbols that had to worn and be visible at all times. This made the Jewish directly visible to the other members of the population limiting their freedom and movements* ***Aid in the mass killings.*** *The biographical information used in the system, lends itself to other purposes. In this particular case, it made it easy to gather and round up the Jewish population aiding in the act of genocide.*									
UK DNA Database	*High*	*Low*	*High*	*Low*	*Low*	*Low*	*High*	*Medium*	*High*	*High*
	Large amount of privacy concerns have been raised. *The DNA is information constantly being accessed without individuals being aware of it. Furthermore it is a highly targeted system that also includes non-convicted individuals. These individuals do not believe they should be on the database, creating a situation of conflict in the creation of the identity. This becomes a major concern since individuals cannot control the presentation of identity to the rest of society.*									

System	*Structural Properties*				*Metrical Properties*					
	Control Points	*Subject Engagement*	*Identity Exposure*	*Population Coverage*	*Subject Coupling*	*Population Comprehension*	*Expert Interpretation*	*Data Accuracy*	*Data Stability*	*Information Variability*
Contact Point	*High*	*Low*	*Medium*	*High*	*Low*	*High*	*High*	*Low*	*Low*	*High*
	Effectiveness of system has been called into question. *Recent cases, such as the death of "Baby P.", have raised doubts on the usefulness of the system. The individual's information being entered into the system is not objective and reduces the accuracy of the data collected. Furthermore, interpretation of results is highly subjective. As the "Baby P." case shows, carers were all aware of each other, but still failed to recognise the trail of abuse.* ***Issues of freedom and self-fulfilling prophecies have been raised.*** *Services that make use of the information may pre-emptively judge an individual and change their modes of interaction. The individual is potentially being assessed on an incomplete picture of his/her identity based on interactions from another context. Furthermore, being targeted at children, such information is not stable and will continuously change, reducing the representativeness of the individual's identity.*									
Austrian Citizen Card	*Low*	*High*	*Low*	*High*	*High*	*Low*	*Low*	*High*	*High*	*Low*
	Low rates of adoption in the digital signature functionality of the Citizen Card. *The system does not present an individual with many opportunities to make use of the identity, creating a lack of perceived benefits. Furthermore, individuals do not understand the system making it difficult to use.*									

5.3.1 Applying the Properties to Other Contexts

To further illustrate the applicability of the properties to different contexts, which in turn acts as a form of verification, the properties will be used to investigate the lived experience of IDMS implemented in non-government contexts. In the following, we apply the properties to a social networking system, and a personalised advertising platform.

5.3.2 Social Networking

Online Social Network Sites (SNS) have experienced significant growth over the past few years. It has become an increasingly popular medium for individuals to connect with each other and share a large amount of personal information. From our point of view, an SNS can be viewed as an identity management system. This makes such sites a prime candidate by which we can apply the codes that the research has uncovered. Specifically, we will be looking at the Facebook platform.

With over 200 million registered individuals, Facebook is arguably the most popular social platform today. It has also been the centre of some controversies. Just recently Facebook has been accused of breaching Canada's Privacy Laws (BBC, 2009). More relevant to our considerations is a change that Facebook made to its website that brought out negative reactions among its community.

In 2005, Facebook introduced new features that affected the way in which information was distributed to an individual's network on the site. Prior to these changes, information that was inserted or updated on an individual's profile was only visible when another party visited his/her profile page. Facebook then added the *Newsfeed* feature, which essentially aggregated all these information changes and broadcast them to an individual's friends. This changed a process from a 'pull' to a 'push' operation. Individuals reacted against this and established resistance groups to voice their opinions. Facebook's CEO eventually responded, stating that no privacy options were taken away, and that the information was visible only to the same people who would have had access before. *"Nothing you do is being broadcast; rather it is being shared with people who care about what you do"* (Hoadley, Xu, Lee, & Rosson, 2009). Nevertheless, Facebook took down the Newsfeed, and re-released it with various privacy controls.

In their study of the situation, Hoadley et al. (2009) attributed the resistance to individuals' perception of *"information access"* and *"illusion of control"*. Individuals viewed the Newsfeed as increasing the ease with which others could access their information, and the absence of controls reduced the level of control that individuals perceived themselves to have. While this point of view is certainly justified, the properties that have been uncovered here might be able to shed more light on the situation and better relate the changes in the system to the reactions.

The most relevant properties for this scenario are the *Control Points* and *Subject Engagement*. Pre-Newsfeed, information was only accessible when another party visited the individual's page. One can technically view this as a single *Control Point*. Post-Newsfeed, the *Number of Control Points* increased dramatically; every party that the information was pushed to represents a *Control Point*, where the individual's information is consumed.

In addition, the Newsfeed can be interpreted as a reduction in the level of subject involvement. In the 'pull' model, visiting an individual's page was a requirement. The page is a representation of the individual on the platform, whom has spent time to create a profile that represents him/her to others. Therefore, accessing the individual's profile page can be seen as a *Control Point* that has high *Subject Engagement*. The Newsfeed represents a loss of involvement, as the information is taken from the individual's controlled profile and broadcast to the other *Control Points* that individuals are not aware of or over which they have no control.

5.3.3 Targeted Advertising

Targeted advertising has proved to be an extremely lucrative way to increase revenues. This form of advertising involves the tracking of an individual's identity across various services. It could be something as simple as contextual targeting (using keywords based on the content of the current page), or based on individuals' browsing history across one or more sites. These browsing histories and identification details are typically handled in a decentralized manner, making use of cookies stored on the user's computer. These tracking methods have raised issues among privacy advocates.

A recent study found that a significant number of the US population object to the tracking of behaviour. Turow, King, Hoofnagle, Bleakley, & Hennessy (2005) found that 86% of young adults reject targeted advertising that tracks behaviour across different websites. Advertisers, however, say that individuals – especially the younger generation – do not mind having their habits tracked. Recent developments in targeted advertising have taken the tracking to new levels.

Phorm is a company that developed a targeted advertising platform that is tied directly to an individual's *Internet Service Provider (ISP)*. Every subscriber to the ISP's network is enrolled into the Phorm system. Every website that an individual visits is passed through the system, and is checked against a list of advertising categories. If a match is found, the category is marked in a cookie and stored on the user's computer. This cookie is then used to provide targeted advertisement on any websites through the use of a widget. The European Union has recently launched legal proceedings in response to the controversial use of Phorm (Wray, 2009). The arguments are usually tackled from a high level law based view of privacy rights. Phorm's representatives argue that people do not understand the technology and how it works, claiming that it actually provides anonymity.

Applying the structural properties from the proposed framework, the items of interest are *Subject Involvement, Identity Disclosure*, and the *Number of Control Points*. With every website passing through the system, Phorm presents individuals with a high *Number of Control Points* resulting in a very restrictive environment for the individual. This situation is exacerbated by low subject involvement at the *Control Points*. The individual's information is taken in a covert manner, without the individual being involved in the process. Phorm also provides individuals with a high *Identity Exposure*. The tracked information is stored on a cookie on the user's computer. In a multi-user environment, the same computer will be used by various individuals amongst whom Phorm will not be able to differentiate. When serving customised ads, the system is constantly at risk of revealing an individual's preference by presenting customised content to the "wrong" individual.

From a metrical standpoint, the properties of interest are in this case are *Subject Coupling* and *Information Stability*. Phorm is a platform used by a user's ISP to deliver targeted advertisements. The relationship between the user and the ISP is that of a consumer paying fees to gain access to the network. This relationship calls for the sharing of certain general and financial information. This is the relevant partial identity of the individual in the subscriber role. By making use of Phorm, ISP's expand beyond this boundary by tracking an individual's habits in depth. This results in low *Subject Coupling* in the ISP-subscriber relationship. Additionally, an individual's browsing habits are constantly growing and producing a very dynamic data set that results in low *Information Stability*. Therefore, in order to keep an accurate representation of the individual, large volumes of up-to-date records are required. This raises concerns of privacy due to the tracking nature of such a system.

5.4 Summary and Discussion

This chapter provides an analysis of a selection of IDMS (based on the systems reviewed in Chapter 2 that resulted in the development of a set of design properties that impacts individuals' *lived experience*. Using thematic analysis, and coupled with the known outcomes for each system, this study outlined a set of *structural* and *metrical properties* that can be used to predict the lived experience offered by an IDMS.

The *structural properties* define the flow of information across the entire identity system, and are captured by the following properties:

1. **Control Points** refer to the volume of points at which a subject's information is accessed or used. A low number of control points imply that the identity is required infrequently throughout the entire life of the identity instantiation.
2. **Subject Involvement** is concerned with the level of participation that the individual has across the various control points. For example, a system that constantly makes use of information at back-end control points, without the subject's knowledge, would signify low subject involvement.

3. **Population Coverage** deals with the percentage of the general population that is actually enrolled into the system. It can be seen as a ratio between the numbers of individuals who are enrolled, against those who are exempt from the system. A highly targeted system would result in low population coverage.
4. **Identity Exposure** defines the level of control that an individual has in the presentation of the identity to other entities that have no right to it. Low identity exposure is one in which the individual has little control of the exposure of the identity to other portions of the population.

The *metrical properties* of an identity system are concerned with the type of information that is captured as well as how the identity information interpreted and used. The following properties are identified as having an influence on the outcomes of an IDMS:

1. **Expert Analysis** refers to the amount of manual involvement of experts that is required to make an identification or authentication. Put in simple terms, it can be seen as the level of subjectivity in the usage or construction of identity. A high level of subjectivity involving specialised skills implies high expert analysis.
2. **Population Comprehension** captures how well the general population understands the identification process and technologies being used. Low population comprehension occurs when the general population does not understand how the identity is constructed and used.
3. **Information Accuracy** defines the reliability of the system consistently to produce correct matches in the practical usage scenarios. A system that doesn't produce any false positives or false negatives is said to have high data accuracy.
4. **Information Stability** is concerned with the frequency with which the subject information being collected changes over time. A system in which the information changes frequently and thus requires constant updating is labelled as having low data stability.
5. **Subject Coupling** is focused on how well the identity instantiation in the system matches the relevant partial identity in the context of use. A system that collects too much or too little information accurately to represent the individual has low subject coupling.

6. **Information Variability** refers to the possibility of the type of information being used for reasons beyond those that it has been collected for. Information such as DNA would have high information variability as various things can be deduced from it, such as medical information, relative identification, etc.

All these properties allow researchers or practitioners to examine how an identity ecosystem can influence outcomes and behaviours of the subjects that have been enrolled into the system. While these properties can be seen in isolation, the real explanatory power of these properties lies in viewing them as a cohesive whole, each influencing and interacting with the others. For example, one can see how a high number of control points, coupled with low levels of subject involvement and low levels of subject coupling, could steer the public to fear an identity system, as has been the case with the DNA database.

5.4.1 Future Work

First off, while the analysis of the work was done until theoretical saturation was reached, a continuous application of these properties to other implementations can serve to further refine the uncovered properties. As an example, it may be beneficial to break down the *Control Point* property into *Read-Only Control Points*, where an individual's information is only consumed, as opposed to a *Write-Only Control Point* where the individual's identity entry is updated with new information. Another possible break down is a distinction between mandatory and voluntary *Control Points*.

Alternatively, new properties can be developed to cover design issues that may not have been brought out in the present analysis. An example of a new property, and one that is currently under consideration, is that of *Information Salience*. This property focuses on the impact of certain metrics in other contexts. Religion for example is a very influential attribute and therefore has a high degree of salience. However, this *Information Salience* property might cause confusion and overlap with that of *Subject Coupling*. It is important to consider the relationship of the new property to the current properties, ensuring that there is no overlap or contradiction. Furthermore, new properties should be valid across different implementations of identity systems.

Another area for further development is the creation of a complete mapping between the individual properties and the potential outcomes that it can bring about. As an example, the analysis here has not identified how high levels of population comprehension might affect the lived experience, and therefore its impacts on the acceptance or rejection of an identity system. One could theorise, and seek proof of a situation where individuals might reject an identity system on the grounds that the population has a complete understanding of that system, thus enabling them to make more informed decisions on what may or may not be acceptable. A complete mapping of the properties to potential outcomes would increase the usability, and hence effectiveness, of the model in describing the lived experience.

Chapter 6: Individual Perceptions of N-IDMS

This chapter outlines a framework that describes individuals' concerns that affect their perceptions and acceptance of IDMS. While the previous study investigated the lived experience of IDMSs (Chapter 5), it does not provide any insight into how individuals develop their initial intentions to trust and accept new IDMSs. The study in this chapter explores individuals' perceptions and thought processes when encountering an IDMS for the first time.

The study presented in this chapter analyses how individuals' initial decision to accept an IDMS is influenced by their perceptions of potential outcomes as a result of the system design. The results of the study show that individuals' willingness to adopt a system is influenced by:

1. **Situation Perception.** The individual's perception of how important the situation being addressed is (Section 6.3.1).
2. **System Judgement.** The individual's assessment of how useful the system will be in tackling the issue (Section 6.3.2).
3. **Concerns.** An individual's concern over the safety of his/her information in the system (Section 6.3.3).

This study consists of three main phases. Firstly, an initial investigation using focus groups to identify concerns, and develop a proposed framework (Section 6.3). Second, a survey based on the proposed framework, was constructed, distributed, and analysed to further refine the framework (Section 6.4.1). Finally, this study also conducted a qualitative exploration of cultural influences on the constructs in the proposed framework (Section 6.5).

6.1 Individual Study

A review of the trust literature reveals that current approaches to predicting trust in a system do not account for individuals risk perceptions (Section 3.3). Current approaches focus on the individuals' general disposition to trust, as well as individuals' context insensitive constructs such as attitude and beliefs. These approaches do not consider the influence that individuals' perception of the system design has on their intentions to trust identity systems; for example, the research has found that individuals' willingness to accept and IDMS is influence by their System Judgement on the usefulness of the identity system, which in turn is dependent on the quality of the information (Section 6.3.2).

The development of a framework that helps to understand individuals' perception of IDMS provides practitioners and researchers with a tool to build more trustworthy systems, which directly address individuals' concerns, thus increasing acceptability.

6.2 Methodology

The individual study used focus group discussions of hypothetical N-IDMS implementations, with the aim being to uncover concerns that individuals have when encountering such systems (Section 4.3.2.1).

Initial pilot studies that made use of one-to-one interviews that proved to be ineffective because individuals seemed to rarely think about identity, privacy, or trust, unless prompted by some kind of negative experience that they can relate to. The subject was not conducive to one-on-one discussions, and thus the interviews quickly devolved into 'interrogations' that produce little interesting data. Based on these initial experiences, it was determined that the study would use Focus Groups to help stimulate rich discussion and shared experiences about individuals' concerns of IDMS (Section 4.3.2.1).

Focus group discussions were further encouraged through the use of scenario-based design as described by Carroll (2000). A set of six different scenarios were developed, each addressing a different policy area that required a hypothetical implementation of an IDMS by a government agency (see Appendix II for detailed scenarios or Table 9 for a summary). The use of a hypothetical implementation was necessary to ensure that all focus group participants, who have been limited to university students (Section 4.3.2.1), were 'exposed' to the same system, and thus enabling all participants to discuss the same topic. Furthermore this also enabled this research to carry out a cross-cultural comparison of the responses of the different nationalities (Section 6.5); i.e. how does national culture influence individuals' responses to the same system. The scenarios provided details of:

1. **A problem that the agency was trying to solve**
2. **A proposed identity system to help address the problem**
3. **A use case scenario that described how the system would work.**

Each hypothetical IDMS differed in terms of the type of information collected, stored, and how it is used. The purpose of this exercise was to determine individuals' concerns in relation to personal information and identity, which could then be extrapolated to various conditions.

Of the scenarios provided to participants, Scenario 6 is the only one that deals with the implementation of an N-IDMS in the traditional meaning of the term, i.e. the use of unique id numbers and identity cards for the whole population. However, the rest of the scenarios still maintain the core issues of N-IDMS, which is the collection, storage, and use of personal identity information by the government.

Further, some of the hypothetical systems in the scenarios may be seen as ambitious in its implementation. However, these scenarios actually encouraged the most discussion, with participants actively discussing the short-comings and improvements to the system. In a way, these scenarios can be viewed as being similar to the concept of *extreme cases* in case study research, which seeks "*to obtain information about unusual cases*", which would produce hypothesis that would "*hold under normal conditions*" (Flyvbjerg 2006).

Table 9 Summary of hypothetical scenarios used in the focus groups to aid discussions

	Situation	Solution
Scenario 1	Child Abuse	Any suspicions of child abuse would be noted into a centralised identity system by carers that came into contact with a child (e.g. doctors and teachers)
Scenario 2	Personal debt	More government control of lending practices. Centralised government system to collect of personal spending and saving information from stores and across all bank accounts. Information used to calculate risk profile each time a loan is requested
Scenario 3	Obesity	Use of CCTV and facial recognition to record food purchases at stores and activity levels at gyms. Information routed to central agency, to determine risk of obesity. Advice provided to those who may be at risk.
Scenario 4	Benefit fraud	Employers enter details of all individuals who are interviewed for a job (commitment, appearance, suitability, etc.) into a central database. Information matched to individuals using fingerprints, and used by government agency to assess if individuals are trying to improve their situation.
Scenario 5	Crime	Collection of DNA from all suspects of a crime, including those who are proven innocent. All recorded DNA is used by authorities to match to crime scene evidence
Scenario 6	Terrorism Illegal immigration	Introduction of identity cards and a national database for the whole population. Cards required to prove identity in various situations from picking up parcel, to accessing government services. Interactions with cards recorded into a centralised database. Law enforcement can access database to investigate security issues.

A total of 15 focus groups were conducted, with the modal group size being 3 participants;2 groups had a total of 4 participants, 9 groups had 3 participants, and 4 groups had 2 participants. Of the 4 groups that had only 2 participants, 1 group was British, 1 was Indian, and 2 were Bruneian. This was largely due to several participants not showing up the focus group sessions, even when 4 participants were scheduled. Research in this case was required to proceed, and did not seem to hamper the study, as the analysis revealed that discussions were just as rich, and that participants debated with one another, while raising similar concerns to the larger groups. Therefore, the research saw this data as being useful for inclusion into the study. While the size of the focus groups were small, this produced discussions that were more productive and rich than those of larger groups of four and above; this is probably due to the complex subject material that required participants to talk in depth about their concerns.

Focus group participants consisted of university students who were of British, Bruneian, or Indian nationality, thus keeping the study in line with the constraints of the organisation study (5.3.1). Each focus group only consisted of participants from the same nationality; of the 15 focus groups, 5 groups consisted of British participants, 5 groups of Bruneian participants, and 5 groups of Indian participants.

The discussions from each focus group, lasting between 60 and 90 minutes, were transcribed, which in total amounted to 115,848 words. The transcripts were analysed using grounded theory (Section 4.3.2.2) to uncover similar thought patterns. During the initial *open coding* phase, codes such as *"using information for fun"* and *"don't mess with the wrong person"* were extracted directly from the transcripts. These type of *in vivo codes* quickly added up, by the fourth group the analysis produced 286 codes. Analysis quickly moved onto the next phase, i.e. *axial coding*, where similar concepts were brought together. In this case, *"using information for fun"* and *"don't mess with the wrong person"*, were combined under the construct of *insiders* (Section 6.3.3), which was then grouped with other similar codes under the construct of *security concerns* (Section 6.3.3). At the same time the analysis carried out *selective coding*, specifying the relationships, between the constructs, around the phenomenon of interest, i.e. the acceptance or rejection of the proposed IDMS. Analysis was done until theoretical saturation was reached, with respect to the data set analysed, and no new codes were being discovered.

6.3 Analysis: Uncovering Concerns from Focus Group Discussions

The grounded theory analysis of the focus group discussions reveal that individuals, from all cultures, may develop their intention to adopt/use IDMSs based on three different aspects of a systems implementation:

1. **Situation Perception**
2. **System Judgement**
3. **Security Concerns**

6.3.1 Situation Perception

An identity system is typically introduced as a support mechanism to address a particular problem; *situation perception* describes how critical an individual believes is found. This is especially true in the case of an N-IDMS, where individuals typically believe that governments should justify their intentions to the public. An individual assesses a problem situation and determines how important it is; the more importance placed on a problem, the more likely he/she will be to choose to adopt the system that will help solve it. These individual assessments are based on three main criteria:

1. **Severity**
2. **Extent**
3. **Exposure**

6.3.1.1 Severity

Severity describes the perceived seriousness of consequences that people might suffer when affected by the problem. Focus group participants rated issues as more serious when there were larger social principles at stake, such as those of equality, fairness, justice, and national security; for example, child abuse, terrorism, and crime are seen as serious issues, when compared to individual problems of health care and personal debt. Therefore, severity isn't just about the implications on the individual him/herself, but is concerned with a moral emotive sense of social good and justice.

Further, severity is not judged for the specific problem itself, but in the context of other problems. At a national level, governments have to manage several different problem issues, each competing for limited resources. Individuals' perception of severity is judged in comparison to these other problems. For example, in *Scenario 4*, one of the participants stated that benefit fraud *"isn't a big problem"*, suggesting that resources be diverted to other issues: *"put more budget on the obesity thing or the child abuse. This will not be a priority" (Focus Group 8 (Bruneian), Scenario 4)*. In contrast to the emotive drivers of severity, individuals also apply a more logical cost-benefit argument in deciding which problems are worth tackling at a particular point in time.

6.3.1.2 Extent

Situation perception is also driven by the assumed *extent* of the problem across the entire population. As the number of people that are affected by the problem increases, the importance of solving the problem is seen to increase. Indian participants thought that personal debt (Scenario 2) was not a problem for many people, and thus saw no need for the proposed identity system. On the other hand, participants in Brunei held a different view, and were more accepting of the proposed solution in the scenario.

> "Participant 1: We need this one. Seriously.
>
> Participant 2: Yeah, definitely.
>
> Participant 1 and 2: Bruneian's are all in debt" (Focus Group 8 (Bruneian), Scenario 2*)*.

6.3.1.3 Exposure

Finally, *exposure* captures the amount of contact or awareness that an individual has to the problem; this can either happen directly from personal experience, or vicariously through the experiences of people they can empathise with. For example, when discussing *Scenario 2*, one of the participants recounted a bad experience with his credit rating, in which someone else's purchasing information was attached to his identity. As a result, he was much more accepting of the proposed identity system involving personal debt, stating *"if it was a government run system, I think it would be an improvement over what exists at the moment" (Focus Group 3 (British), Scenario 2)*. Similarly, participants who had experience working with children such as Bruneian students doing an education curriculum, as well as two British participants who have experience with Family Law, were more aware of related issues, and were typically more inclined to agree that a solution needed to be found when tackling issues of child abuse.

Indirect experience of the problem can come from media reports. Problems that are highlighted in the news expose individuals, making perception of the problem more salient, and thus more important to solve. In response to the child protection scenario, the British focus groups regularly referred to television or newspaper reports, and how the current procedures are shown not to work. When discussing personal debt, the Bruneian groups frequently touched on recent media coverage that outlined a speech from the Sultan criticising the Brunei Islamic Religious Council (BIRC) regarding the distribution of *Zakat* (alms) to people in need *(Focus Group 7 (Bruneian); Scenario 4)*; at the time, BIRC was still in possession of BND$230 million of undistributed funds (Brunei Times, 2009).

6.3.2 System Judgement

In addition to *situation perception*, an individual's initial acceptance of an identity system may be influenced by his/her overall judgement of the effectiveness of the IDMS in helping to tackle the stated problem. *System judgement* is a deduction that an individual makes based on his/her understanding of how the system works. An individual's deduction about a system appears to be developed based on four different areas of consideration:

1. **Information Relevance**
2. **Information Accuracy**

3. **Information Reliance**
4. **Outcomes**

6.3.2.1 Information relevance

One of the core components to system judgement is individual's perception of the relevance regarding the information collected, to the goals of the agency. Participants would make negative judgements of the IDMS if they thought that the information being collected was irrelevant to the problem situation or organisation. The focus groups show that *information relevance* is influenced by:

1. **Granularity**
2. **Sensitivity**

Granularity refers to the level of detail being collected and stored in the IDMS; i.e. it refers to the amount/depth of information that is collected. Collecting too detailed personal information is seen as overstepping boundaries. When discussing *Scenario 2*, participants who favoured the system stated that collecting details on every single purchase would be intolerable. They suggested that information collection be minimised, and limited to general categories of data (e.g. luxury items); in doing, so the *granularity* of the information collected is reduced to acceptable levels. *"… if on the point 4, it was just a simple cash flow, non-itemised, I think it would be good, cause it would help banks develop better risk profiles for people. So, good in that regard. Anymore, and I sort of get a bit uncomfortable." (Focus Group 1 (British), Scenario 2).*

Sensitivity captures how private nature the information is to the individual. The more sensitive the information, the more individuals will judge it to be irrelevant. When discussing *Scenario 1*, participants raised concerns about deductions that teachers may be able to make about a child's medical condition from the doctors notes in the system. The inverse issue was never raised, indicating that the notes that teachers make are seen to be less sensitive, and therefore more acceptable.

Sensitivity and *granularity* are not mutually exclusive; a better understanding of relevance can be obtained when considering how the two interact with one another. The more specific the information becomes, the closer it is to the individual's private boundaries, and therefore the more sensitive it becomes. Similarly, the greater the perceived *sensitivity* of the information collected, the more critical individuals tend to be about the *granularity* of the information.

6.3.2.2 Information Accuracy

System judgement is also influenced by the overall accuracy of the personal information collected, stored and used. Individuals' perception of inaccurate information, developed through their assessment of the overall data collection protocol, negatively affects the final judgement of the usefulness of the system. Through the focus groups, three main factors are believed to influence perceptions of *information accuracy*:

1. **Subjectivity**
2. **Completeness**
3. **Visibility**

Firstly, there is the concern about *subjectivity* in the information collection phase. Situations in which information is not 'objectively' captured, but is generated by third parties, are seen to reduce accuracy. There is the perception that these parties may exaggerate or influence the information according to their personal preferences, thus producing inconsistencies between different external parties. These concerns show themselves in *Scenario 4*, where employers' notes about an individual's appearance are deemed to be a subjective construct that is influenced by the employer's personal preference; *"It is especially bad in the case thing, how the employer is interviewing and makes notes, especially on appearance. That is one person's opinion" (Focus Group 1 (British), Scenario 4)*. Thus, inconsistencies are created where no two employers would produce similar comments on the exact same appearance of an individual. Similarly in *Scenario 1*, several groups believed that the notes made by carers regarding suspicions of abuse would only create a database of inaccurate rumours. In these cases, participants proposed reducing subjectivity by introducing a quantifiable measures or proper guidelines, thus providing a perceived element of objectivity to the information.

Completeness is another concern; all focus groups raised the issue that the system would not be able to collect all the required information specified, and thus would produce an inaccurate representation of the individual in that particular context. For example, in *Scenario 3*, participants pointed out that the system would not be able to track all the physical activities of an individual; the individual might do exercise outside the monitored gym environment, thus producing an inaccurate representation of the individual's activity levels. Similar concerns were raised in *Scenario 2*, where it would be impossible to track every single purchase from every single store, thus reducing completeness.

It seems here that there is some *tension* between the individuals' perception of *granularity* and *completeness*. On the one hand, individuals are not comfortable in the organisation collecting too much detail, but on the other hand are also concerned about the organisation not capturing enough information to develop an accurate representation. Some distinction can be made between the two concerns in that *completeness* deals with the specific points of data collection, while *granularity* deals with the specific information collected at each of these points. Nevertheless these tensions still exist, and system designers should be aware of these potential conflicts that need to be resolved.

Lastly, *visibility* refers to the accessibility of the targeted personal information by parties other than the individual to whom it pertains; the more visible the information, the easier it is for an external party to notice and record that information; the less visible the information is, the more individuals believe that there will be inaccuracies, as there are gaps in the knowledge. This concern is especially prevalent where information needs to be noted without the subject's co-operation or awareness (*subjectivity*; see paragraph above). In *Scenario 1*, the issue of child abuse is something that is not directly visible. As a result, not only are the notes about children considered subjective, but participants also believed that the lack of visibility would lead to further inaccurate notes that sensationalise the information. *"Child abuse is hidden. It is hard to know when it's just completely innocent. It is a big step for teachers to say: Oh look, there is a bump there, so there must be abuse" (Focus Group 1 (British), Scenario 1).*

6.3.2.3 Information reliance

A third factor that may influence *system judgement* is the degree to which organisations come to rely on the information collected and stored. *Information reliance* highlights the individual's perception of how relevant parties will utilise their personal information to inform their decision making process when interacting with the individual. The perception of reliance is mediated by:

1. **Dependence**
2. **Challenge**

Focus groups were concerned about organisations sole *dependence* on information stored on the IDMS. When organisations become too reliant on the stored information, they stop seeking out other sources of information that individuals believe would lead to more appropriate outcomes. For example, a common conclusion in *Scenario 2* was that the loan decisions would not produce good results, because the system does not collect the varying reasons for each loan application (business ventures, etc.). In *Scenario 4*, the welfare agency would only make decisions based on the information provided by employers. It was suggested that the agency not rely on this single source, but should seek out more information, such as mental health status, to ensure that proper action is taken.

Here, there is another source of *tension*; one between the *dependence* and *relevance*. While individuals are deeply concerned about the organisation over stepping its boundaries, they also believe that the organisation should also collect varying types of information so as to come to informed judgements. So again, designers need to be aware of these subtle conflicts within individuals' perception of the system.

Lastly, focus group participants were concerned about the ability of an individual to *challenge* the information that leads to decisions made about him/her. This issue was most prominent in *Scenario 5*. Participants saw the use of DNA to be deterministic, in that they perceive it to be too difficult to challenge one's identification as a criminal. The most common solution proposed was to create mechanisms to ensure that the DNA information collected would not be used as evidence of a crime, but instead as indicators to pursue further investigation, thus reducing information reliance, while increasing an individual's ability to counter the claims.

6.3.2.4 *Outcomes*

Along with *information relevance*, *accuracy* and *reliance*, an individual's *system judgement* may be mediated by the perceived *outcomes* of the system implementation. *Outcome* is generally expressed as the overall effects that the system has on society; this can materialise as issues of:

1. **Freedom**
2. **Fairness**

Issues of *freedom* are commonly tied to issues of tracking that are seen to erode personal liberties; individuals feel like they are constantly being watched, and will thus be reluctant to act freely. For example, the use of CCTV in stores and gyms in *Scenario 4* is seen as a highly judgemental system, which places a psychological burden on the individual to change his/her behaviour, so as to fit the expected norm. These perceived attacks on freedom negatively influenced individuals' perception of the system. In *Scenario 4*, one participant claimed *"she would rather leave the country than be exposed to the system"*. Furthermore, many participants claimed that weight management was a personal choice, and should not be imposed upon people, unless they specifically requested for that level of control in the first place. Similar views were expressed in some discussions about *Scenario 2*, where financial management is considered a personal right that should be free from government control.

Fairness covers issues of potential discrimination, and the creation of a tiered society. In *Scenario 4*, most participants were against the idea of using the information collected to reduce free medical support for obese individuals who fail to lose weight. The argument put forward was fairness; obese people were singled out, while people suffering from other self-inflicted health problems, such as smoking, are not. One group claimed that in order to ensure fairness the system would also have to adjust medical benefits for those who choose to do extreme sports, and are therefore more prone to injury.

6.3.3 Security Concerns

In addition to the *situation perception* and *system judgement*, willingness to adopt an identity system is mediated by individuals' *concerns* about the security of their personal information in the system. The concerns identified related to issues of:

1. **Unauthorised Access.** Participants raised concerns about the systems security and hackers gaining access to the system. For example, one participant stated, "*the biggest fear I have is that, unless you have a closed network, you are going to open that system up to the web. That becomes a huge target. Not only hackers, but even other countries to attack*" (Focus Group 3, British, Scenario 6). In another focus group a participant was concerned about "*the possibility of someone going into your system, hacking and changing information… we are not there yet*" (Focus Group 7, Bruneian, Scenario 6).
2. **Insiders.** Participants were concerned about corruption, and thus abuse of their personal information by people who have legitimate access to the system. The concerns were centred on the use of the identity against the individual, for insiders' personal gain. As explained by a participant, *"I do not mind if my DNA is collected, but it has to be used only for crime, not just for fun. It would likely happen. Maybe the officer hates me or something, trick the system, into making others think I did something bad."* (Focus Group 6, Bruneian, Scenario 5). Similarly participants in India echoed these concerns who frequently stated and agreed that "*there is a lot of corruption in India",* and that *"you cannot really trust the government employees, they just like to make a quick buck if they could. If they could use that footage in some way, which would help them, they would. They wouldn't think about it twice"* (Focus Group 12, Indian, Scenario 4).

3. **Future Unpredictability.** Focus groups raised concerns that the information collected can be used for other unknown purposes, by future governments that might come into power. This issue dealt with function creep and governments' ability to resist from using information that they have for entirely different purposes. *"Well, I think if it was possible to contain a DNA database for the specific use of crime then it might be worth while doing. But I think now, it probably wouldn't be limited to that. It's probably the way that the DNA would be used for other purposes. That makes it a risk. For the right crime, it's probably a good idea. I don't know that much, but I fear that it wouldn't be limited to just that."* (Focus Group 1, British, Scenario 5). In another group, discussion on the use of fingerprints for the purposes of benefit fraud, a participant expressed the belief that the system *"can be used for other things. It is more likely to be a wider criminal database. The pressure to use it to do that… government will submit to pressure of function creep"* (Focus Group 3, British, Scenario 4).

6.4 Proposed Framework for the Citizen Perception of Identity

Using the results of the focus group analysis, a model for the development of initial citizen perception and acceptance of an IDMS can now be created (Figure 16). From the analysis, the three major antecedents to the initial acceptance appear to be:

1. **Situation Perception.** Situations and problems perceived to be important will create a more accepting attitude towards a new IDMS.
2. **System Judgement.** Positive perception of the effectiveness of an IDMS will also generate more positive attitudes.
3. **Security Concerns.** High levels of concern around the security of personal information would have a negative impact on the acceptance rate**.**

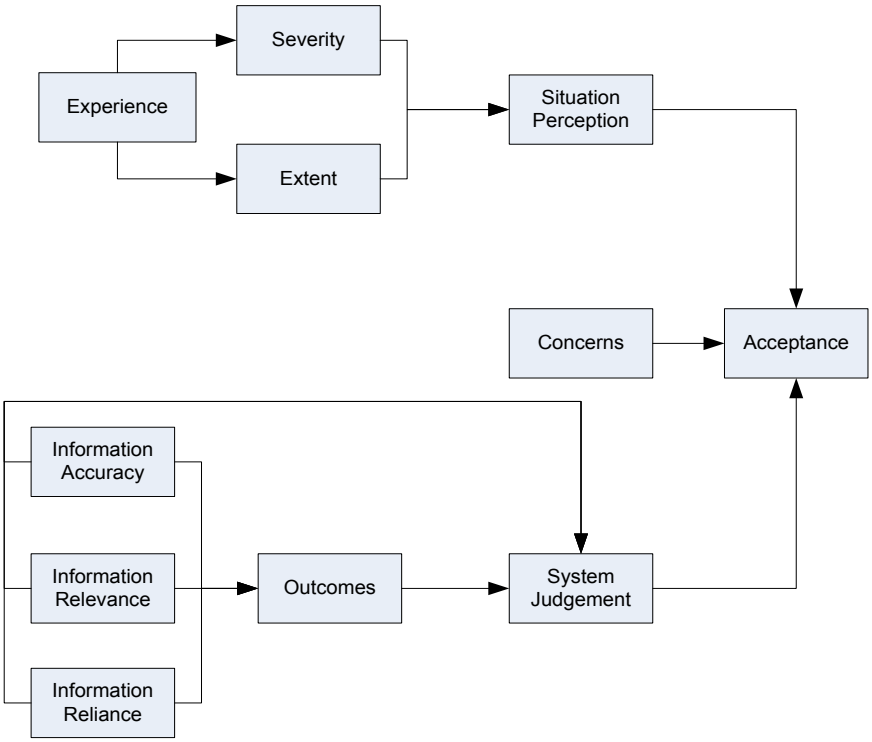


Figure 16 Proposed Citizen Perception framework based on analysis of focus groups

Severity and *Extent* are hypothesised to be antecedents to *Situation Perception*. The perceived importance of addressing a particular problem is positively influenced by the seriousness of the problem being tackled, as well as the extent of the population affected by the problem. Individuals' perception of *Severity* and *Extent* are further influenced by their exposure to the problem; having had some kind of experience or awareness of the problem may inflate individuals' attitudes regarding the seriousness of the problem, and the number of people affected by it.

System Judgement is based on individuals' perception of information being collected and how it may be used; it is influenced by *accuracy*, *relevance*, *reliance*, and *outcomes*. Systems that are perceived to hold inaccurate and irrelevant information are seen as an ineffective tool or resource for an organisation. Furthermore, a perceived strong reliance by the organisation on the information in the system is seen to lead to inflexible and mechanical responses from the organisation, thus generating a negative response to the IDMS.

The overall *outcomes* also influence the individuals' views of the system; a large number of negative outcomes may be perceived to create a more problematic situation. *Outcomes*, dealing with issues of fairness and freedom, are influenced by the type and amount of information collected; therefore, like *system judgement*, *outcomes* are influenced by *accuracy*, *relevance*, and *reliance*.

6.4.1 Survey Study: Improving the framework

Based on the analysis and hypothesised theoretical framework from the focus groups, the study used quantitative methods to confirm the relationships between constructs to examine and improve the *fit* of the model.

The survey was designed so as to focus on the higher level constructs identified within the model (see Appendix III for survey questions); e.g. questions items were only developed to focus on the issue of *information relevance* itself, and not on its sub-constructs (i.e. *granularity* or *sensitivity*). This limitation was introduced so as to keep the length of the survey down to a manageable size; the inclusion of questions relating to each of the nine sub-constructs identified would have drastically increased the length of the survey, negatively affecting completion rates. Several question items were developed to operationalize each of the constructs under investigation; these questions were constructed and refined through discussions and informal evaluations with colleagues and acquaintances, as well as a very small pilot study within the department. Every item was measured on a 4-point scale (*Strongly Disagree, Disagree, Agree, and Strongly Agree*), so as to ensure a positive or negative response to each question.

The study made initial attempts to pre-test the survey by distributing a recruitment email to all Computer Science students within the University College London (UCL); participants were entered into a luck draw to win £50. However, this received very low response rates, with only a total of only 13 participants. Therefore, due to time limitations, the research had to resort to individual walkthrough of the survey with 6 different participants, consisting of other research colleagues who have designed surveys, as well 4 acquaintances that have no background in research. The result of the walkthrough test showed that all participants understood the questions, with only very minor changes to the wording of the questions. The other concern raised through the walkthrough with research colleagues was with respect to the length of the questionnaire. However, the responses received from the Computer Science students showed that all participants who participated completed the survey, indicating that the survey was able to hold participants attention till completion of the survey.

After pretesting, the survey was distributed online to a random sample of students from the University College London. This was achieved by sending an email out to a UCL wide mailing list that targeted all undergraduate students. Each survey participant was entered into a lucky draw for a prize of £50. Based on the 13,772 undergraduate students enrolled in UCL at the time the survey was distributed (UCL Registry & Academic evices, 2012), this represents a 4.85% response rate. Participants were first required to read *Scenario 1*, outlining the implementation of an IDMS that aimed to tackle the issue of child abuse.

Analysis of the data occurred in a two-step procedure; *Exploratory Factor Analysis (EFA)* was first used to test the measurement model, ensuring that all question items loaded onto the appropriate construct. This was then followed by the use of *Structural Equation Modelling (SEM)* to test the structural model, which deals with the relationships between the constructs. It is typical operating procedure that the same dataset not be used for both EFA and SEM. To accommodate for this, the responses obtained from the survey were randomly split into two data sets (using SPSS software package), containing 320 and 366 responses respectively.

6.4.1.1 Exploratory Factor Analysis

EFA is a procedure that is typically used to understand the underlying structure of a set of variables (Field, 2009). It calculates the correlation between each variable; groups of variables that correlate highly among each other indicate that those variables are measuring aspects of the same underlying factor. EFA was used here to ensure that the question items developed loaded onto the relevant constructs while diverging from the other constructs.

Using SPSS 19 software for windows, EFA was applied onto one half of the randomised dataset. Principal Components was used as the extraction technique; initial EFA applications used an eigenvalue threshold of one to extract underlying factors. Varimax rotation was used to maximise the loading of questions onto a single construct, to help improve interpretation of the data.

The results of the initial EFA extracted a total of eight factors, which is less than the 11 constructs predicted in the proposed framework. Based on the rotated component matrix (see Appendix IV), the analysis found that:

1. ***Severity* and *Situation Perception* question items loaded onto a single factor**
2. ***Relevance* and *Accuracy* question items loaded onto a single factor**
3. **A few *Reliance* question items loaded onto the combined *accuracy/relevance* factor.**
4. **Remaining *Reliance* items and a majority of the *Judgement* items loaded onto the same factor.**

In light of these unexpected factor loadings, a confirmatory approach was adopted in which the expected number of factors was specified; i.e. 11 factors to reflect the 11 expected constructs. All 11 factors extracted were observed to *Eigenvalue* of 0.865 or more (Table 10), which is still above the widely accepted *Eigenvalue* of 0.7 (Field, 2009).

Table 10 Factor Analysis of all question items with 11 factors specified

	Initial Eigenvalue			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.583	26.619	26.619	4.894	13.596	13.596
2	3.188	8.855	35.474	3.698	10.271	23.867
3	2.247	6.241	41.715	2.604	7.233	31.100
4	1.940	5.388	47.103	2.401	6.670	37.770
5	1.596	4.432	51.535	2.103	5.842	43.612
6	1.394	3.873	55.409	1.836	5.100	48.712
7	1.137	3.158	58.567	1.801	5.003	53.715
8	1.004	2.789	61.356	1.576	4.377	58.092
9	.969	2.692	64.048	1.467	4.076	62.167
10	.930	2.583	66.631	1.262	3.505	65.672
11	.865	2.402	69.032	1.210	3.360	69.032
12	.769	2.136	71.168			

However, the results of the confirmatory factor analysis were unsatisfactory, in that certain question items still loaded unexpectedly onto different constructs (see Appendix IV); in particular one *extent* and *judgement* question item loaded onto a single factor, while one *accuracy* question item loaded onto the *acceptance* factor. To address this issue, the study took an exploratory approach to examine the strength of variable loadings onto unexpected factors. The corresponding question item was reviewed, and compared to the other question items with which they correlated; similarities in the questions would explain the unexpected loadings, and in these situations two initially separate constructs may in fact be collapsed into a single construct. On the other hand, unexpected loadings in which the question is not related to the other correlated questions, and thus have no theoretical reasoning, would imply that the variable should be eliminated.

Using this iterative process, items that only loaded strongly onto a single factor on its own, without any theoretical basis, were removed from the data (see Appendix IV). A total of 10 question items were removed; including all the items relating to the *outcome* construct.

Also to be noted is that the *severity* and *situation perception* question items still loaded onto a single factor, as did the remaining *accuracy* and *relevance* items. Furthermore, *system judgement* and *use* items now also loaded onto the same factor.

To further explore these loadings, separate EFAs were conducted on the development of *situation perception*, and the development of *system judgement*. These are two different processes that are based on different aspects (situation vs. system), and therefore it would be beneficial to explore the factor loadings of the corresponding question items in isolation of each other. An EFA analysis was applied onto the question items that correspond to *situation perception* and its antecedents (*experience*, *severity*, and *extent*). Similarly, EFA analysis was also run on the variables corresponding to *system judgement* and its antecedents (*accuracy, reliance, outcomes,* and *judgements*).

EFA on the situation constructs, based on Eigenvalues of one, produced similar results to previous test, where *situation perception* and *severity* question items still loaded onto a single construct. However, taking a more confirmatory approach, and using PCA to extract four factors (min. Eigenvalue = 0.743), *severity* and *situation perception* question items did in fact load onto two separate factors, implying the existence of the two separate constructs. The initial loading of the two constructs onto a single factor might be explained by the fact that *severity* is an antecedent on *situation perception*, and therefore are strongly correlated to each other.

On the other hand, a confirmatory approach on the *system judgement* process did not present any new insight. Thus, *accuracy* and *relevance* constructs were collapsed into a single construct called *information quality*. The theoretical underpinning of this decision was that both original constructs dealt with the process of information collection and storage.

On a similar note, the remaining *use* and *judgement* variables still loaded onto the same factor. Going back to the survey reveals that the *use* question items dealt with the impacts of using the identity information to inform organisational decisions; this is theoretically similar to the remaining *judgement* items that deal with the effectiveness and usefulness of the overall system. Therefore, informed by the factor loading, and the theoretical similarity of the question items, the remaining *use* items were collapsed under the *judgement* construct.

Table 11 Factor loadings of all question items. Factor Analysis (PCA). Minimum Eigenvalue of 1. Varimax rotation.

	Component						
	1	2	3	4	5	6	7
acc3	.771						
acc2	.720						
acc4	.720						
acc1	.690						
sev2		.751					
per1		.751					
sev3		.686					
sev1		.677					
per2	.419	.658					
per3	.514	.651					
con1			.807				
con4			.758				
con3			-.700				
con2			.676				
jud1				.756			
jud2				.673			
use3				.641			
use1	.437			.500			
acu3					.788		
acu1					.755		
rel2					.643		
rel3					.442		
ext1						.813	
ext2						.788	
exp1							.774
exp2							.769
exp3		.447					.567

Table 10 shows the factor loadings under rotation, after the removal of unsatisfactory variables; factors were extracted on the basis of a minimum eigenvalue of 1, and weak loadings of less than 0.4 were suppressed for easier reading. The clustering of variables around factors fit the following constructs:

- **Factor 1 represents *acceptance***
- **Factor 3 represents *concerns***
- **Factor 4 represents *judgement* (*use* variables subsumed under *judgement*)**
- **Factor 5 represents *information quality* (*accuracy* and *relevance* collapsed together)**
- **Factor 6 represents *extent***
- **Factor 7 represents *experience***

Factor 2 in Table 11 shows the combined loading of *severity* and *perception* items onto a single factor. Table 12 shows the factor loadings of items that are related to the development of *situation perception* only. From the table, *situation perception* and *severity* can be seen to load onto two different factors, factor 1 and factor 2 respectively.

Table 12 Factor loadings of situation perception, severity, extent, and experience question items. Principal Components Analysis. 4 factors specified. Varimax Rotation

	Component			
	1	2	3	4
per2	.848			
per3	.845			
per1	.790			
sev3		.784		
sev1		.760		
sev2	.470	.677		
exp1			.847	
exp2			.733	
exp3		.405	.602	
ext1				.871
ext2				.749

The factor loading matrices also enable us to establish the validity of the survey instrument and measures. Validity is a necessary prerequisite for successful development of a model, ensuring that the instrument measures what it was designed to. This mainly consists of *convergent validity* that refers to the extent to which the variables posited reflect a given construct converge, and *discriminant validity* that refers to the extent to which variables that make up a construct differ from those that are not believed to make up the construct.

Analysis of the factor loadings shows that most measures load highly onto their respective factors, having factor scores of greater than 0.5, with the majority being in the range 0.65 to 0.8. The exception to this is *rel3* that has a factor score of 0.442, which is still close to 0.5. These results provide evidence for convergent validity.

Analysing the tables for cross-loadings of question items to different factors shows that the variables do not load strongly with any other factors; where cross-loadings do exist, it does not exceed the loading of the variable onto its original factor. Furthermore, the factor score co-variance matrix shows that each factor is independent of one another (Table 13). Together these figures establish the discriminant validity of the measures.

Table 13 Factor Score Covariance Matrix after iterative EFA. Extraction Method. Maximum Likelihood

Factor	1	2	3	4	5	6	7
1	.952	.000	.000	.000	.000	.000	.000
2	.000	.850	.000	.000	.000	.000	.000
3	.000	.000	.751	.000	.000	.000	.000
4	.000	.000	.000	.744	.000	.000	.000
5	.000	.000	.000	.000	.704	.000	.000
6	.000	.000	.000	.000	.000	.629	.000
7	.000	.000	.000	.000	.000	.000	.598

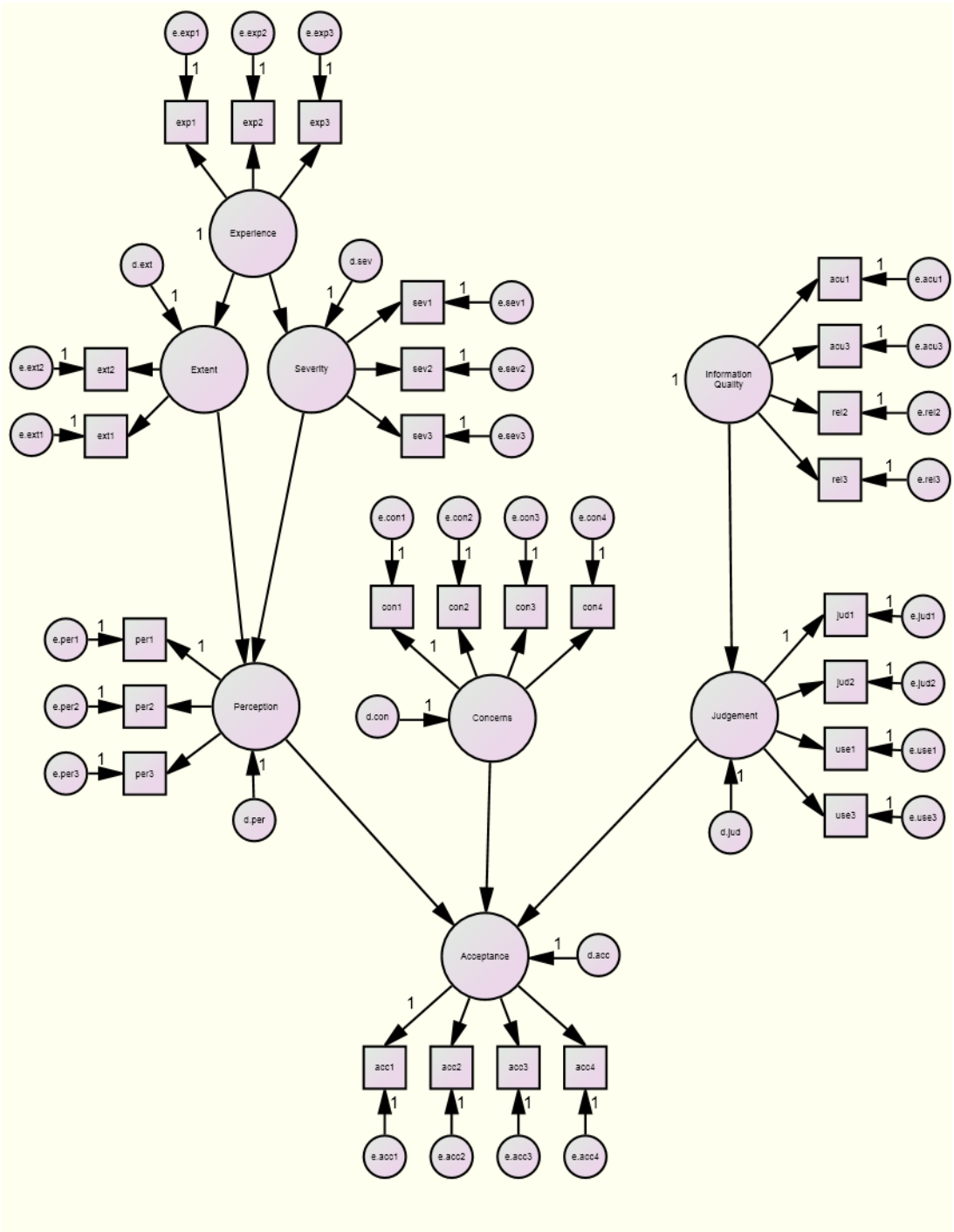
Validity is a necessary but not a sufficient condition of a measure. Reliability must also be considered, ensuring that the measures can be interpreted consistently across different conditions. Reliability can be tested by calculating the value of Cronbach's alpha for each measure. Values of 0.7 or 0.8 for Cronbach's alpha are considered a good measure of reliability, while scores below 0.7 may also be accepted when dealing with psychological constructs. Analysing Cronbach's alpha for the factors shows that all constructs have high levels of reliability, with alpha being greater than 0.7. However, *experience* has a value of 0.6, and extent a value of 0.647, both of which is still within acceptable levels.

Table 14 Cronbach Alpha values for factors identified through the survey

Construct	*Cronbach's Alpha*
Perception	*0.863*
Experience	*0.6*
Severity	*0.763*
Extent	*0.647*
Information Quality	*0.728*
Judgement	*0.807*
Concerns	*0.773*
Acceptance	*0.878*

6.4.1.2 Structural Equation Modelling

Once EFA was completed on the measurement model, and constructs confirmed for reliability and validity, SEM was used to assess the fit of the structural model, analysing the correlations of the constructs against each other. AMOS 19 was used for the SEM process, where the proposed model was specified (accommodating for the merging of factors described in Section 6.4.1.1); constructs were set up as latent variables, while each item corresponding to that construct was set up as an observed indicator of that variable (Table 17)



Chi-square	*Normed Chi-Square*	*GFI*	*AGFI*	*NFI*	*CFI*	*RMSEA*
820 *p = 0.000*	*2.598*	*0.858*	*0.831*	*0.821*	*0.881*	*0.66*

Figure 17 Proposed individual perception model constructed in AMOS to test fit

The model was analysed in AMOS using maximum likelihood as the estimation procedure. The suitability of the model is evaluated by assessing the various measures of fit produced. Table 15 shows the most commonly cited fit measures, and their critical values for interpretation. The more fit measures that fall within acceptable ranges, the more confident one can be of the model fit.

Table 15 Commonly used fit statistics in SEM (Abramson, Rahman, & Buckley, 2005)

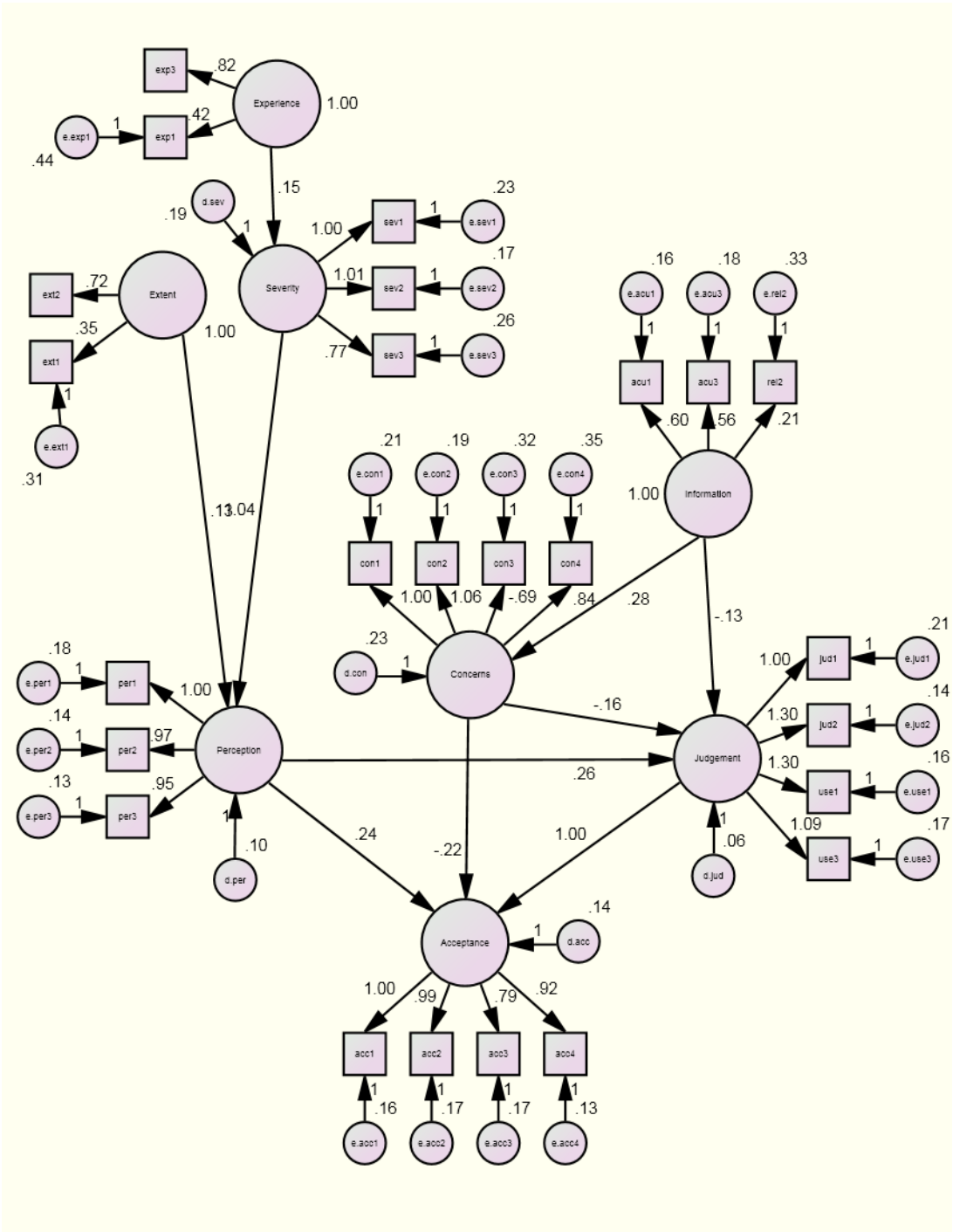
Test Statistics	Critical value	Interpretation
Chi-squared Tests		
1. Chi-squared goodness of fit test	Chi-squared = n.s.	Good fit to the just-identified model.
2. Normed chi-squared test	Chi-squared/df <=3	Good fit to the just-identified model.
Test Statistics Using Covariance Matrix		
1. Goodness of fit index (GFI)	0.9 < GFI < 1	Good fit to the just-identified model.
2. Adjusted goodness of fit index (AGFI)	0.9 < AGFI < 1	Good fit to the just-identified model.
3. Standardized root mean squared residual (SRMR)	0 < SRMR < 0.05	Good model fit.
Comparisons with Independence Models		
1. Normed fit index (NFI)	0.9 < NFI < 1	Percent improvement over null model
2. Non-normed fit index (NNFI) [aka the Tucker-Lewis Index]	0.9 < NNFI < 1	Percent improvement over null model
3. Comparative fit index (CFI)	0.9 < CFI < 1	Percent improvement over null model
Root mean square error of approximation (RMSEA)	0 < RMSEA < .08	Good model fit.

The analysis of the proposed model produced fit measures that fell outside the acceptable range, with only the normed chi-square and RMSEA statistics providing an indication of good fit. Following this, the study adopted an exploratory approach to produce a better fitting model. Fit measures assess how well the parameter estimates produced by the model, account for the co-variances observed in the data set. While the initial model that was developed through the focus group analysis produced two fit statistics within acceptable ranges, the model re-specification brought other fit-measures within acceptable ranges, thus providing the research with greater confidence that the re-specified model accounts for all the observed co-variances; i.e. the re-specified model is a more accurate reflection of reality.

This model re-specification involves the adding or removal of variables, and can be aided by the use of residual matrices and modification indices produced by AMOS (Abramson, Rahman, & Buckley, 2005). This was an iterative process, involving the removal or addition of single variables or correlations (that have theoretical basis) to analyse its effect on the overall fit of the model; the adjusted model produced is illustrated, along with its fit measures, in Figure 18.

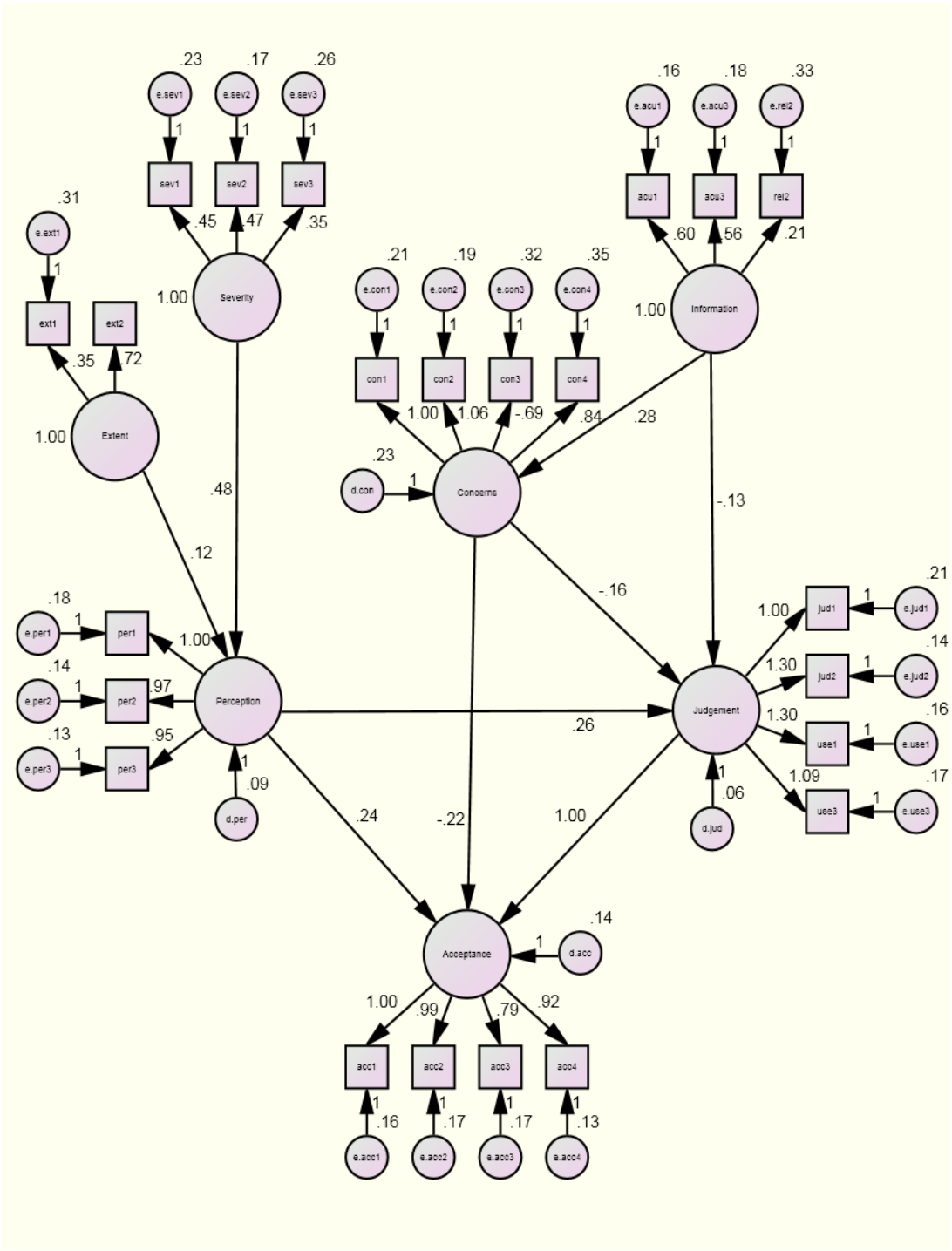
The Model Fit indices for the adjusted model show that this is a better model than that originally proposed, with the normed chi-square, GFI, CFI, and RMSEA all indicating a good fit. Based on the modification indices produced by AMOS, new theoretically justifiable relationships were added to the model. *Information quality* is placed as an antecedent to *concerns*, as this constructs deals with the security of information within the system. *Concerns* in turn act as a direct antecedent to *system judgement*; having high concerns over the security of the personal information would have a negative impact on the judgement of the overall system. *Situation perception* also acts as an antecedent to *system judgement*; the more urgent a situation is perceived to be, the more the judgement of the system will be a positive one. Lastly, *exposure* was removed as an antecedent to *extent*.

Finally, attempting to produce a better fitting model, simple multiple regressions was used to explore the relationships in isolation. The findings from this showed that while *experience* had a statistically significant relationship with *severity*, the strength of the relationship was very weak (0.067). Removing the *experience* construct from the overall model in AMOS, increased NFI to 0.9 indicating a good model, while also increasing the AGFI to 0.893 (Figure 19); this indicates that the final model produced is a better fit when compared to the second adjusted model (Figure 18)



Chi-square	*Normed Chi-Square*	*GFI*	*AGFI*	*NFI*	*CFI*	*RMSEA*
268 *p = 0.000*	*1.763*	*0.907*	*0.887*	*0.890*	*0.949*	*0.046*

Figure 18 Improved individual perception model based on SEM process



Chi-square	*Normed Chi-Square*	*GFI*	*AGFI*	*NFI*	*CFI*	*RMSEA*
222 *p = 0.000*	*1.789*	*0.914*	*0.893*	*0.902*	*0.954*	*0.046*

Figure 19 Final individual perception model after experience construct is removed

6.5 Analysis: Cultural Factors Affecting Acceptance

Apart from the general constructs that lead to the acceptance or rejection of an identity system, the study also investigated the influence of national culture on acceptance. Focus groups were designed such that participants in each group were culturally homogeneous, sharing the same nationality, thus allowing for a comparison of responses across these three cultures (i.e. Bruneian focus groups, British focus groups, Indian focus groups).

Hofstede's national culture values (Section 3.4.2 and Section 4.3.2.3) were used to establish the cultural differences between each of the three countries. While the cultural measures of British and Indian focus groups were readily available (Geert Hofstede et al., 2008), measures from Brunei were not. Therefore, the cultural value measurement survey was distributed to undergraduate computer science university students in Brunei (University of Brunei Darussalam). However, these Bruneian measures are not directly comparable to the published British and Indian results, as they are based on unmatched samples; *"comparisons of countries should be based on matched samples of respondents: people who are similar on all criteria other than nationality that could systematically affect the answers"* (Hofstede et al., 2008).

A possible way around this limitation is to *anchor* the new results to the available measures by distributing the survey to one other country of which the values are already known. *"Anchoring means that the scores from the extension research should be shifted by the difference of the old and new scores for the common country"* (Geert Hofstede et al., 2008). As such, the study distributed the Value Survey Module (VSM) questionnaire to undergraduate computer science students in Britain; specifically students from the University College London; the VSM is a publicly available questionnaire, provided by Hofstede, to measure National Culture (Hofstede et al., 2008).

A total of 21 Bruneian and 22 British students replied to the survey, which is within Hofstede's minimum recommendations (Hofstede et al., 2008). The anchored cultural measures are listed in Table 16.

Table 16 Cultural value measures for countries under investigation

	PDI	IND	MAS	UA	LTO	IVR	MON
Brunei	*84*	*41*	*56*	*88*	*79*	*39*	*(57)*
UK	*35*	*89*	*66*	*35*	*51*	*69*	*(25)*
India	*77*	*41*	*56*	*40*	*51*	*26*	*(-)*

A limitation of the cultural inquiry is the small number of countries under investigation; according to Hofstede (2001), quantitative use of the cultural measures *"demands data for a large number of countries, preferably 10 or more; qualitative use is possible for any comparisons of two or more cases"*. Therefore, the cultural investigation here seeks to qualitatively explain the variances in responses between participants of each country, based on the discrepancies in the cultural scores, and their implied effects as described by Hofstede (2001).

The investigation has uncovered several affects that national culture has on the acceptance of IDMS:

1. **PDI correlated positively with concerns for information abuse**
2. **IDV correlates positively with concerns of freedom**
3. **IDV correlates positively with concerns of function creep**
4. **UA correlates positively with concerns over security**
5. **UA correlates positively with acceptance (low protest potential)**
6. **LTO correlates negatively with information quality (information is more sensitive)**
7. **LTO correlates positively with acceptance (focused on the growth of the country)**

6.5.1 Power Distance on Concerns of Information Abuse

"Power Distance is defined as the extent to which the less powerful members of institutions and organisations within a society expect and accept that power is distributed unequally" (Geert Hofstede et al., 2008). In High PDI societies, the powerful tend to exert their power and maintain their positions, while the weaker individuals accept the power gap. As a result, high PDI societies tend to have citizens that distrust authorities, and also tend to have higher occurrences of corruption (Hofstede, 2001).

Brunei and India both rate highly on the PDI scales (84 and 77 respectively), when compared to a Britain (35); this discrepancy in the scores appears to reflect the concerns of individuals when assessing an N-IDMS. Bruneian and Indian focus groups were highly concerned about *corruption* and the *abuse* (see Section 6.3.3, as well as the direct quotations provided below, that emphasise the concerns of participants) of information by insiders.

Indian participants felt uneasy about having all that information in the hands of the government, specifically mentioning *corruption*, and how information could be used against them by those in power.

> *"Interviewer: But you also raised issue about do you trust the authorities and do you trust …?*
>
> *Participant 1: Yeah.*
>
> *Interviewer: Could you expand on that some more.*
>
> *Participant 1: Yeah. Well, okay, like bringing in all these other factors like the politicians having their own problems and their own past crimes, whether their information will actually be correct or not. It's possible that my DNA is mixed with yours, or like switched with yours just because of carelessness or just because of problems with the structure itself. Maybe that would be a problem, maybe purposeful changes made to the data. That could be a problem, so it's just, I don't know if it's safe in the hands of someone like the police. Maybe like people have mentioned, maybe high profile cases sure, but not necessarily everyone.*
>
> *Interviewer: Does everybody agree with that?*
>
> *Participant 2: Yeah, at the moment the DNA should be kept in the hands of the police. I don't think that it should be a case if this is implemented in India because the police can't be trusted" (Focus Group 13 (Indian), Scenario 5).*

Bruneian participants also had concerns of abuse by *insiders* (Section 6.3.3), but were less focused on the higher political corruption issues; instead, concerns centred on *insiders* who might use stored personal information for personal attacks against the individual, and *"exploit this data, for their own use" (Focus Group 9 (Bruneian), Scenario 6).*

"Participant 2: For example, anyone apart from the carers, have access to that information. They can use that information to perhaps sabotage the parents. I think that would be a problem" (Focus Group 7 (Bruneian), Scenario 1).

"Interviewer: Do you trust the government to protect your information?

Participant 2: That is quite blurry.

Participant 1: In Brunei…

Participant 2: It depends. If you don't mess with the wrong person" (Focus Group 8 (Bruneian), Scenario 3).

On the other hand, British participants did not explicitly raise issues of corruption issues. It was only mentioned implicitly when suggesting that proper access and security protocols would provide the necessary security for the identity information.

6.5.2 Individualism, Freedom and the Future Unpredictability

"Individualism stands for a society in which the ties between individuals are loose: a person is expected to look after himself or herself and his or her immediate family only. Collectivism stands for a society in which people from birth onwards are integrated into strong, cohesive in-groups, which continue to protect them throughout their lifetime in exchange for unquestioning loyalty" (Geert Hofstede et al., 2008). A consequence of this is that the principle of equality among individuals becomes an important point for individualist societies. Hofstede (2001) notes that IDV is positively correlated to a country's human rights ratings. High IDV societies also tend to strongly believe that everyone has a right to privacy.

Britain scored highly on the IDV scale (89). Compared to the more collectivist societies of India and Brunei (IDV score of 41 for both countries), British participants more frequently raised issues around *future unpredictability* (Section 6.3.3) of the personal information, constantly mentioning issues of tracking, being pressured from acting freely; this confirms the importance of privacy and human rights within highly individual societies.

"Participant 1: If it was to suffer from the same problems as the last one, the with the, uh, sort of, not believing people can make the right decision of their own accord. It's really not, like, respecting their ability to make decisions. It seems to be a bit like… and also people have a right, people have a, it's their choice if they want to be, if they want to be overweight and not do exercise. Fine. If they want that. That's fine.

Participant 2: I think there's nothing wrong in promoting a healthy lifestyle. I think that is good, I think we have to do it in the, like when we study we have to do health promotion and, but there are different ways of doing it and I think this isn't really a good way. I don't think that people would find this encouraging. I don't think that people would take it… like, I want to be healthy but I would never, I don't think I could ever, I don't know, what's it called?… Do this. No, I, I wouldn't apply to this, I'd be very reluctant. So I think that it's obviously targeting a good thing but no I'd find it really hard. It's too much monitoring. I don't want to be monitored 24 hours, no" (Focus Group 2 (British), Scenario 3).

In a similar vein, British focus groups were highly concerned about *function creep*; information being collected and stored would be used for other purposes. Again, this taps into human rights issues where the information is used in new ways that potentially invades privacy and freedoms, creating unequal relationships between citizen and state.

"Participant 1: I was just going to say that this goes a bit further than the idea of a credit rating. This is actually, checking out what you are buying. Which as long as you don't go into debt and don't pay off your debts, you buy what you want, don't you?

Participant 2: I do ponder as well. It says, it will track information, purchasing habits, but if you are buying cash, I don't see how it can track. If you are paying cash over a debit card, then I am not entirely sure, will that shopper who makes a lot of cash transactions, and then, hey if I am making a lot of cash transactions, is it because they are doing illegal stuff? It's this danger of creep. You can have one thing and then have someone who is taking out a lot cash and say, 'Why is this person buying in cash? Are they a drug dealer? What is going on?' The problem is, it starts off with innocent and positive effects, but could quite easily slip into creep" (Focus Group 3 (British), Scenario 2).

In contrast, participants from India and Brunei rarely brought up freedom principles, and function creep took a back seat in the discussions, only ever mentioned implicitly. These results are in line with Hofstede's observation that collectivist societies tend to have lower human rights ratings, and accept states where *"private lives are invaded by public interests"* (Hofstede, 2001). In certain cases, especially the Bruneian context, there was some recognition of the privacy invasions, but was seen as less important when compared to the greater good.

> *"Participant 1: Child abuse is something you don't talk about in public. You have to dig deep down to know. The child won't say anything. It is up to the carers, the teachers, and doctors, to notice.*
>
> *Participant 2: Maybe it should not be accessible for the employees, just for the doctors, the police officers, things like that.*
>
> *Participant 1: Yes. Input information, but not access what others commented about that child. I wish we can have this here.*
>
> *Participant 2: I am thinking about those kids" (Focus Group 8 (Bruneian), Scenario 1).*

6.5.3 Uncertainty Avoidance on Security and Acceptance

"Uncertainty Avoidance is defined as the extent to which the members of institutions and organisations within a society feel threatened by uncertain, unknown, ambiguous, or unstructured situations" (Geert Hofstede et al., 2008). Hofstede (2001) found that uncertainty avoidance was negatively correlated with confidence in the civil service, and willingness to protest.

From the focus group discussions, Bruneians tended to voice concerns over the security of the system; government was seen as being unable to sufficiently defend against attackers breaking into the system, i.e. *hackers* (Section 6.3.3). This was less evident in the British and Indian groups, and is explained by Brunei's comparatively high score on the UAI measure (88 to Britain's 35 and India's 40).

Additionally, the Bruneian focus groups were less likely to express strong resistance or outright rejection of the scenarios. Rejection of a system was commonly expressed as the system being *"annoying"* (Focus Group 6 (Bruneian), Scenario 3), or that *"it would not be a nice thing to do"* (Focus Group 7 (Bruneian), Scenario 3). This is in contrast to Indian participants who expressed stronger arguments about why an identity system should not be implemented; British participants were the most vocal in their rejections, sometimes stating that they would protest, or would *"just go to a country where they don't have it (the identity system)"* (Focus Group 5 (British), Scenario 3).

6.5.4 Long-Term Orientation on Sensitivity and Acceptance

"Long-Term Orientation stands for a society which fosters virtues oriented towards future rewards, in particular adaptation, perseverance and thrift. Short Term orientation stands for a society which fosters virtues related to the past and present, in particular respect for tradition, preservation of 'face', and fulfilling social obligations" (Geert Hofstede et al., 2008). As LTO is a relatively new dimension to the cultural survey, there are not many connotations attached to it; however, according to Hofstede (2001) *"high LTO families tend to keep to themselves"*.

Brunei scores highly on LTO (79), while India and Britain have comparatively low scores (both scoring 51). This difference manifests itself in the Bruneians' approach to determining *information sensitivity* (Section 6.3.2.1) and its impact on privacy; Bruneians didn't see privacy as being only about the individual, but as also extending to the individual's social circle; breaching an individual's privacy is seen to have an impact on the family unit as well. This concern is further emphasised by common arguments relating to the small size of the country, where in *"Brunei, everyone knows everyone"* (Focus Group 10 (Bruneian), Scenario 1). India and British participants did not share the same concerns, and privacy was judged on an individual level, rather than the social level.

However, LTO might also have an impact on the overall acceptance of an identity system. Although Hofstede has not investigated the impacts of LTO beyond family and business, the focus group indicate that LTO could have a positive impact on the willingness to ensure for the long-term security of the country. It was common for Bruneians to express acceptance of an IDMS they might not entirely agree with, citing the importance of growth and development of the country. These arguments were absent from the Indian and British focus groups.

> "*Interviewer: Do you think the public would be accepting of such a system?*
>
> *Participant 2: I myself, if I was a parent, I would want that. It means that the country is advancing; they should be open to such things" (Focus Group 7 (Bruneian), Scenario 1.)*
>
> "*Participant 1: Even though I don't agree with… stores might give false information, etc., but I 90% agree that this will reduce the number of people being in debt in Brunei" (Focus Group 8 (Bruneian), Scenario 2).*

6.6 Summary and Discussion

A focus group study was conducted to explore individuals' perception and acceptance of IDMS. Grounded theory analysis revealed that individuals' willingness to accept an IDMS is depends on 3 main constructs. Based on the above findings, a proposed model for acceptance of an IDMS was developed that had each main construct serve as an antecedent to acceptance, which in turn was dependent on its sub-constructs:

1. **Situation Perception** describes the urgency with which a problem needs to be addressed.
    a. **Severity** touches on the seriousness of being affected by the problem.
    b. **Extent** captures the frequency of the problem among the population.
    c. **Exposure** accounts for the experiences and awareness that an individual has to the problem.
2. **System Judgement** describes the individual's perception of how useful the system will be in helping to address the problem.
    a. **Information Accuracy** captures the individuals' perceived accuracy, completion, and subjectivity of the information being collected and stored.

b. **Information Relevance** captures the individuals' thoughts on the relevance, sensitivity, and granularity of the information being collected and stored.
c. **Information Reliance** captures the perceived dependency and flexibility of the organisation in using the information to make decisions.
d. **Outcomes** capture the general societal outcomes in terms of freedom and fairness.

3. **Security Concerns** describes the individuals' fears over the security, safety, and abuse of the identity within the IDMS**.**

Using the proposed model and constructs, a survey was developed to quantitatively explore the hypothesised relationships between the major constructs. The survey was distributed to all undergraduate students at the University College London, and received a total of 668 completed responses. Based on the 13, 772 undergraduate students enrolled in UCL at the time of the survey , this represents a 4.85% distributed (UCL Registry & Academic evices, 2012).

Exploratory Factor Analysis (EFA) showed that *information accuracy* and *information relevance* loaded highly onto the same factor; these were then collapsed into a single factor called *information quality* dealing with the overall concerns about the information being collected and stored. EFA further showed that most of the *outcome* items loaded highly onto *judgement*. Referring back to the survey, the respective questions items all touch on concepts similar to the *judgement* construct. This may indicate a need to develop new questions for the *outcomes* construct so as to avoid any overlap. To proceed with the quantitative investigation, the *outcomes* construct was removed from the model, while merging the relevant items into the *judgement* construct.

Overall the factor loadings showed that items loaded strongly onto a single factor, with little cross loadings onto other factors. An exception is the *severity* and *situation perception* construct; however, this is unsurprising as *severity* is predicted to be an antecedent to *situation perception*, and is thus expected to correlate to some extent. Isolating and running EFA on *situation perception* and its antecedents showed that *severity* and *situation perception* do load onto separate constructs; thus, divergent and convergent validity is achieved across all factors. Cronbach's alpha was used to show the reliability of all constructs, all of which had a value of above 0.6, the majority of which were in the range of 0.7 and 0.8.

Structural Equation Modelling (SEM) was then used to explore the model and relationships between each construct. Initial analysis based on the proposed model produced unsatisfactory fit statistics. Through an iterative process, based on the SEM results, as well as sound theoretical reasoning, new relationships were added or removed from the model. A well-fitting model was produced where:

1. **Experience was eliminated from the model**
2. **Information Quality was an antecedent to Concerns**
3. **Concerns was an antecedent to System Judgement**
4. **Situation Perception is an antecedent to System Judgement**

In addition to the general acceptance model, the study was also designed to investigate the effects of national culture on the overall perception, and willingness to accept an IDMS. Focus Groups were designed so that all participants in each focus group came from one particular country; five British focus groups, four Bruneian focus groups, and five Indian focus groups. Due to the small number of countries investigated, the effects of national culture could only be described qualitatively. This was done using Hofstede's cultural value measures and the implied effects that he has captured and described (Hofstede, 2001).

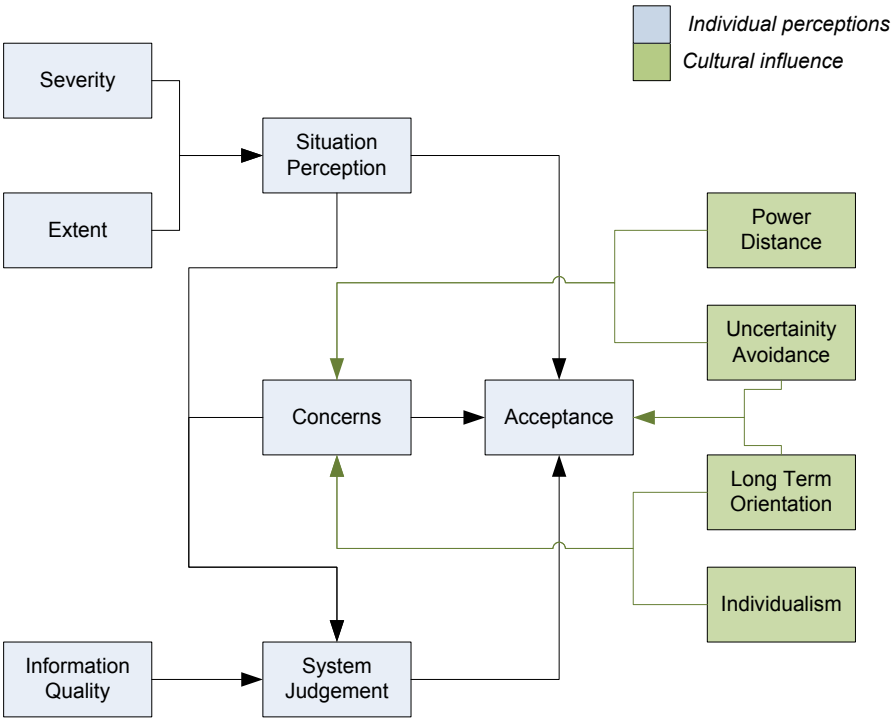


Figure 20 Final individual perception framework, including culture

Using the results from the grounded theory analysis, discrepancies between responses from the different countries were noted, and linked to the cultural score values. The study has found that *power distance, individualism, and uncertainty avoidance* serve as antecedents to security concerns; with each measure respectively heightening issues around abuse, unpredictability, and ability of government to secure information. On the other hand, *long-term orientation* serves as an antecedent to *information quality*, where long-term orientated societies tend to have a more social view of privacy, and therefore see information as being more *sensitive*.

Finally, *long-term orientation* and *uncertainty avoidance* both have a positive relationship on the *acceptance* construct; long-term orientated societies place the development of countries above personal concerns, while high uncertainty avoidance countries reduce their willingness to protest, thus increasing the likelihood of acceptance.

Overall these findings indicate that individuals' perception of IDMS is largely focused on the outcomes of the system. How will the situation be improved? Are the right problems being tackled? Will the system be useful and effective in solving the problem? Will insiders and hackers abuse the identity information? These findings are in line with other privacy research that has found that individuals are focused on consequences, as opposed to traditional informational privacy dimensions. (Paine et al., 2007) showed that Internet users' privacy concerns were focused on issues viruses, and *hackers*. Similarly, Weirich (2001, 2005) found that individuals concerns over following security measures were influenced by their perceptions of hackers gaining access to the system. Adams's (2001) work in multimedia communications found that privacy invasions happen when due to the transmission of sensitive information, as well as its unexpected usage. Further, the proposed framework does have some similarity to that of Smith's traditional informational privacy measures (Smith et al., 1996). For example, the originally proposed constructs of *granularity* and Smith's *collection* construct, as well as the proposed *information accuracy* construct and Smith's *error* construct. However, the framework developed here extends beyond Smiths' standalone constructs, as it is used as an antecedent to determine individuals' *system judgement*.

6.6.1 Future Work

The *individual acceptance* framework broke away from the traditional trust research in order to identify how the IDMS itself influences intentions to adopt. Having done so, it may be beneficial to extend the findings incorporate trusting elements to increase the explanatory of the framework.

Using Pavlou (2003) and Malhotra, Kim, & Agarwal (2004) as a foundation, we begin to see how risk can be integrated into the trusting model as described by Li (2004). Pavlou (2003) showed that perceived risk influences trusting intention, while trust is an antecedent to both trust and risk (Figure 21). Malhotra et al. (2004) also demonstrated that risk beliefs affect trusting intention, and further illustrated that the risk beliefs are influenced by privacy concerns regarding the information collection and control, as well as the sensitivity of the information collected (Figure 22).

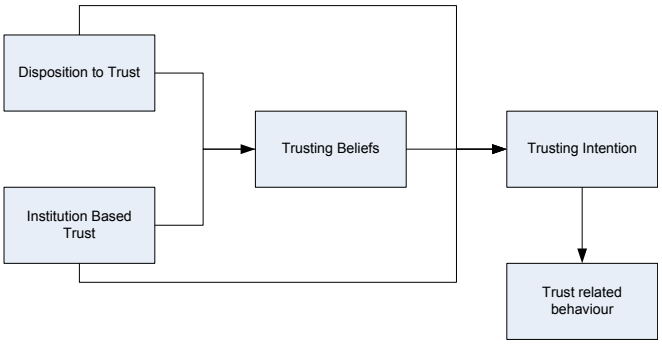


Figure 21 Pavlou (2003) Trust-Risk model

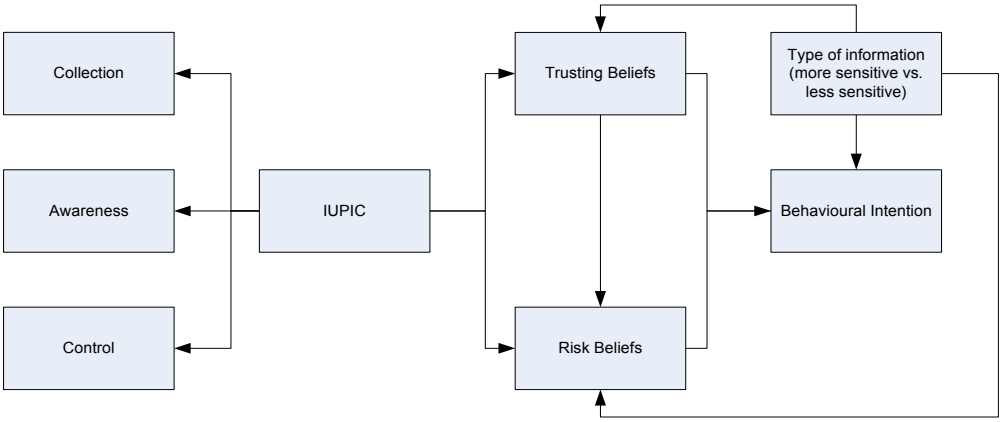


Figure 22 Malhotra et al. (2004) IUPIC model

Meanwhile, the findings of individual acceptance framework appear to align themselves with the concept of risk; for example, *concerns* over the security of the information, or the severity of the problem if left unattended, resonate with the concept of risk. Therefore, future work might hypothesise and place the constructs of the individual acceptance framework as an antecedent to the individual's perceived risk of an identity system, which is determined by an his/her system assessment, problem evaluation and security concerns. Thus, based on the above two models, it may be possible to combine the individual acceptance framework with Li's (2004) comprehensive N-IDMS trust model, as shown in Figure 22.

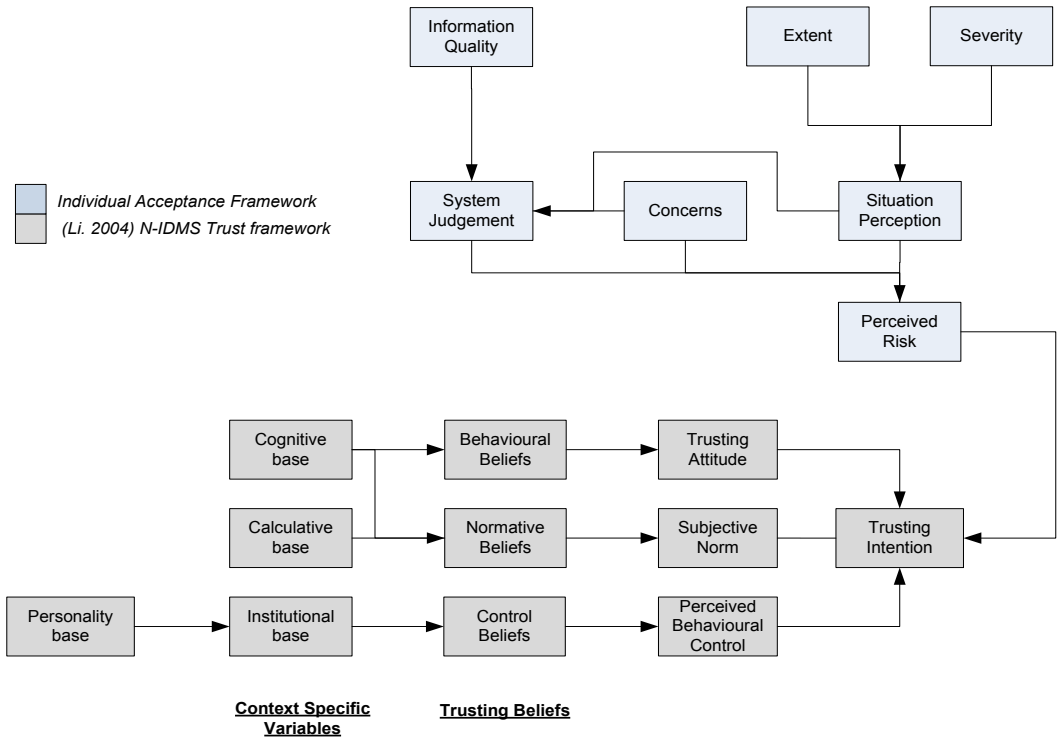


Figure 23 Proposed trust-risk framework for IDMS

Chapter 7: Organisation Perspective on the N-IDMS

This chapter describes a framework that captures organisations' identity requirements, and guides the design and implementation of an IDMS.

The literature review in Section 3.5 revealed that most research into organisations and IDMSs have focused on identity as an authentication mechanism to access secured resources. However, as it is used today, identity has moved beyond security, and has itself become a resource.

The research presented here explores identity as the strategic resource being accessed; it explores the influences of organisational identity requirements on the design and implementation of an IDMS. This study investigated the implementation of N-IDMS in 3 different countries; Brunei (Section 7.2.1), UK (Section 7.2.2), and India (Section 7.2.3). Using interviews, and publicly available government documents, data collection was focused on organisations arguments for the system, as well as the corresponding strategy and design of the N-IDMS to fulfil those goals.

Using Grounded Theory, the analysis found that organisational identity requirements are driven by the overall *purpose* of the system (Section 7.4), which in turn affects two major processes that organisations are concerned with; *identity construction* (Section 7.3.1), which is focused on maintaining the integrity of identities within the system, and *identity use* (Section 7.3.2), which is focused on the access and use of identity.

7.1 Organisation Study

While the previous two studies focused on the system and the individual respectively, the third and final research study focused on the organisation implementing an IDMS. In recognising the organisation, discovering the organisation's identity requirements, and how these affect the planning and implementation of an IDMS.

By investigating identity as a strategic resource, this study constructed a framework that captures the organisational requirements and its implications on the design of an IDMS. The formalisation of these requirements into a framework can help designers build identity systems that are fit for purpose, while also helping to inform policy debates, by highlighting the areas of concern, as well as reducing ambiguity in the discussions.

7.2 Methodology

The study presented in this chapter used a case study approach (Section 4.3.1) across three different N-IDMS implementations, each in a different country; Brunei, United Kingdom, and India (Table 17). The investigation drew from various qualitative sources that were available in each context, ranging from interviews to publicly available government documents.

7.2.1 Case Study 1: Brunei Darussalam

Documentation on the current Bruneian N-IDMS case was not readily available. There are only a handful of articles that cover the history of the system; these were used to describe the development of the system since its inception. Therefore, to support the main analysis of this case study, interviews were conducted with several different government agencies that have been involved in the implementation and use of the system. Interviews were conducted with:

1. **Brunei National Registration Agency (BruNIR).** The lead agency and owner of the Bruneian N-IDMS. This key interview session involved the director of the BruNIR along with two other high-level government officers that were involved in the development, and on-going use of the system.
2. **Information Technology Protective Security Services (ITPSS).** A company that handles various security aspects of the identity system, and other e-Government projects.

3. **Tabung Amanah Pekerja (TAP).** TAP, which is in charge of the national retirement fund, is one of the few organisations that have adopted the multi-use functionality built into the N-IDMS smart cards.
4. **Land Transport Department (LTD).** Initially seen as prime candidates to ride on top of the BruNIR N-IDMS. However, current plans to upgrade the LTD system include plans to introduce their own stand-alone identity and smart card system.

7.2.1.1 System development

Brunei Darussalam, located on the island of Borneo in South East Asia, and has had an N-IDMS for the past 63 years. The first paper-based identity cards, which contained a photograph and personal details, were introduced in 1949 under the authority of the Police Force (Yunos, 2009). This responsibility was later subsumed by the BruNIR in 1965, which introduced new forms of paper ID cards that made it easy to distinguish between citizens, permanent residents, and temporary residents (Brunei Immigration & National Registration Department, 2005). The system was later upgraded again in 1975 to include the collection, storage, and display of rolled fingerprints.

In 2000, the BruNIR chose to modernise its identity infrastructure. Upon enrolment, which is compulsory for any citizen over the age of 18, personal details and digital copies of each individual's biometrics (facial and fingerprint) are recorded, and stored on a centralised database (Yunos, 2009). A unique identifying number is generated for each individual, who is then provided with an identity card. Intending to create an environment to support the development of eGovernment, the BruNIR chose to use smartcards that contained a chip holding a digitised version of the individual's personal information, as displayed on the card, as well as a digital template of the individual's fingerprints.

Table 17 Summary of the N-IDMS analysed in the study.

	Brunei	India	Britain
Date Implemented	2000 – today	2010 – today	2008 – 2010 (abandoned)
Purpose	Multi-function smart card	Support poor in accessing services	Prevent terrorism, crime, benefit fraud, travel card
Mandatory	All residents (18 and above)	Volunraty for all Indian residents	Mandatory for high risk personnel; airport staff, etc. Voluntary in early stages, with eventual plans for it to be mandatory for everyone.
Unique ID Number	Yes	Yes	Yes
Identity Card	Yes	Yes	Yes
Smart Chip	Yes	No	Yes
Centralised Database	Yes	Yes	Yes Specifically, the system will make use of three separate databases - one for biometrics - one for biographical information - one for PKI data.
Authentication (Against Card)	Yes	No	Yes
Authentication (Against Database)	No	Yes	Yes Audit log of transactions
Information Read	Third Parties can access biographical information on card and chip.	Third parties can confirm the accuracy of information (yes/no response only).	Third parties can access biographical information on card and chip. Security organisations can get access to all information on the database (through information commissioner).
Information Write	Third parties can to write to the smart card	None	Information can be pushed from third parties to the database.

7.2.1.2 Adoption

Although the distribution of the smartcard to the total eligible population was completed by 2001, the uptake of the digital authentication and multifunction use of the smartcard has stagnated. TAP is the only local third party organisation that makes use of the smartcard; it is used as an authenticator that allows an individual to check the balance in their retirement accounts at specific kiosks (Brudirect, 2002).

Additionally, the BruNIR has recently entered agreements with neighbouring Malaysia, enabling both countries to use their respective smartcards as passports at land borders; respective immigration agencies in each country are able to authenticate, read, and write information against the chip (Razak, 2007; Said Ya'akub, 2007).

However, in spite of these developments, many public and private organisations continue to use the identity smart card only as a physical proof of identity, while also stating that there were no limitations placed upon the use of the unique identity numbers provided to each individual (Interview with BruNIR).

7.2.2 Case Study 2: United Kingdom

Due to the long running controversies that led to the eventual demise of the UK N-IDMS, the present study was unable to secure interviews with relevant stakeholders from the Identity and Passport Service (IPS). While some early indications for interviews proved promising, they never materialised; the study also attempted to hook onto the PVNets project, which conducted privacy investigations on the IPS passport system, but this avenue also did not lead to any interviews with the organisation.

However, unlike the Bruneian context, official documentation on the system was more readily available. Although the documentation did not contain specific technical details, it was rich in the strategic arguments on the need for an N-IDMS, and its potential uses. Other material was also available in the form of research publications and media relations, both of which were used to support analysis where needed; specifically when building the historical background of identity development in the country studied (Section 7.2.1.1 and 7.2.2.1), as well as to refer to key influential critiques of the N-IDMSs under investigation (primarily the [London School of Economics, 2005] report on the UK N-IDMS that is referred throughout this section).

7.2.2.1 System development

In the past, the United Kingdom had implemented and managed two identity systems, during World War I and World War II respectively (Agar, 2001); both systems were scrapped soon after each war. The World War I system was used to aid in the process of conscription, enabling the government and military to count the number of able-bodied individuals who could take up arms (Elliot, 2006). The system fell into disuse once it had fulfilled its purpose.

The identity system established in WWII was set up as an access mechanism for the distribution of rations to the public. The system survived through the end of the war, as rations were still being distributed. Recognising the value of an N-IDMS for efficiency, and that the need for rations would soon expire, the government attempted to attach other *parasitic* value to the N-IMDS by integrating the use of identity cards into the health and insurance schemes (Colvin & Spencer, 1995). However, the system faced much resistance from the public, who rejected the *prussianizing* aspects of an N-IDMS, failing to update their records as needed (Agar, 2005). This all culminated in the case of John Wilcock who was arrested when he refused to present his identity card to the police. Mr Wilcock's case was taken to court, where the judge sided with Wilcock, which eventually led to the decommissioning of the WWII identity system.

Recently, the British government has attempted to introduce an identity card. As with previous systems this was done under their premise of National Security, claiming threats from terrorism. Other justifications that the government put forward for the need of an N-IDMS included organised crime, illegal immigration and benefit fraud (London School of Economics, 2005). The current approaches of proving identity, where individuals regularly make use of various third party documents (e.g. banks or utilities), were argued by the government to be insufficient to tackle these issues. A stronger identity system controlled by the government was claimed to assist governments in addressing the stated problems.

Furthermore, international developments around travel documents were also used as an argument to support the introduction of an N-IDMS. For example, the United States was in the process of adopting and mandating the need for biometric identifiers in travel documents (U.S. Senate, 2002). Additionally, the Schengen agreement between 25 European nations (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Norway, Iceland and Switzerland) allowed individuals to travel between each country using only an identity card (European Commission Home Affairs, 2010). Therefore, in addition to its national security goals, the N-IDMS was also positioned as an ideal platform by which it can abide by the new standards being adopted in travel documentation (London School of Economics, 2005).

The government introduced the Identity Cards Act in March 2006 ("Identity Cards Act," 2006) that provided the legal framework for the establishment of the IPS to implement and manage an N-IDMS. The act called for the introduction of an identity card supported by a database, the National Identity Register (NIR). Anyone over the age of 16 was required to enrol with the IPS, by attending an interview session, providing 50 different categories of biographical information, as well as providing biometric information (*Identity Cards Act*, 2006). In November 2008, IPS began rolling out compulsory identity to foreign nationals entering the country. Voluntary enrolment was eventually opened to residents of Greater Manchester in November 2009, which was followed by enrolment of air industry staff at London and Manchester airports (Identity and Passport Service, 2009, 2010).

7.2.2.2 Functionality

Identity systems by their nature both enable and disable individuals from carrying out some form of action. However, following the pattern of reasoning adopted by the UK government, their intention for introducing the N-IDMS seemed to be on the exclusionary power of identity; the focus on prevention can be seen to materialise in the early enrolment strategies that target high risk populations, such as airport workers and foreigners (Identity and Passport Service, 2008).

The UK N-IDMS was designed to support both online and offline authentication of identity (Identity and Passport Service, 2006). Offline authentication using the identity card was designed to work in two ways; firstly, there was the simple visual check of the individual against the facial photograph printed on the identity card; secondly, using a card reader, the relying party could check the fingerprint of the individual against the biometric template stored on the chip. Online authentication was also available, where the fingerprint and card details would be routed to the IPS and checked for authenticity ensuring that the card was real and the fingerprints matched.

In addition to the authentication capabilities, the UK N-IDMS also supported information sharing. This can be initiated by the individual through the use of the identity card, enabling a third party to read the data stored in the card. The system also supports the push of information to third parties when an individual updates his/her information in the database (Identity and Passport Service, 2006). Alternatively, the IPS also specified back-end approaches to sharing information. Supported by its anti-terror goals, the N-IDMS has mechanisms that enable security organisations to access personal information stored on the database; the individual is never notified of this access, and would remain unaware that his/her information had been accessed (Blunkett, 2003; *Identity Cards Act*, 2006).

7.2.2.3 Adoption

Although implementation began in 2009, roll out of the N-IDMS was never completed due to a change of government; the new Conservative/Liberal Democrat coalition was opposed to the introduction of an N-IDMS (BBC, 2010a). Additionally, public perception had shifted; while initial polls in 2003 showed that the public was in favour of ID cards (61% for, 38% against, 1% neutral), a follow up poll in 2006 showed a decline in public support (46% for, 51% against). Privacy campaigns, such as NO2ID, regularly voiced their opposition to the system. Media coverage became highly critical of the planned N-IDMS, as were researchers working in diverse fields from security, to privacy, and public policy (for example, see London School of Economics, 2005). Within this landscape, the new government announced the abolition of the N-IDMS, and introduced a new bill that would cancel all existing identity cards, and the destruction of data held on the N-IDMS database (Home Office, 2010).

7.2.3 Case Study 3: India

The Indian N-IDMS forms the third and final case study. As with the case in the UK study, the research into the Indian N-IDMS was not able to secure interviews with the relevant stakeholders. Contact was made through the Science and Innovation department of the British Deputy High Commission in Bangalore; the request for interviews was forwarded to the UIDAI, who showed interest, but failed to follow up; in response to the request, the contact in the Science and Innovation department stated that *"the Identity Card project representatives are keen to work with international researchers but they don't have a proper mechanism or protocol for it right now"*. However, as with the UK study, the Unique Identification Authority of India (UIDAI) has made available documentation outlining its strategy, and the integration of its services with various public and private services; these materials formed the basis of the investigation into the Indian N-IDMS.

7.2.3.1 System development

India does not have much experience with N-IDMS, and a large section of the poor population do not possess any form of recognised identity; while no exact figures on those without identity documents are available, (Unique Identification Authority of India, 2010a) states that the N-IDMS intends to register up to 1.079 billion individuals that make use of social welfare services in the rural areas. This has largely led to the development of fragmented identity schemes across different areas, where the proof of identity varies between regions or between service providers. Consequently, the poorest and most needy part of the population have been unable to access various welfare services, such as the Public Distribution System (PDS), the National Rural Employment Guarantee Scheme (NREGS), public health, and financial institutions among others. The shifting requirements of identity and the general lack of documentary proof have made it too difficult and expensive for the poor population to claim or prove their identity (Unique Identification Authority of India, 2010a).

The lack of an identity infrastructure means that organisations are unable to track the proper distribution of goods and services to those who are entitled to them. Furthermore, the current identity approach is also believed to facilitate corruption, as organisations are unable to effectively identify who may be siphoning resources that they do not have a right to. (Unique Identification Authority of India, 2010b, 2010c).

Thus, the Indian government has been keen to introduce an N-IDMS. Attempts in 1993 and 2003, saw the distribution of identity cards by Election Commission, without any national database or identifiers. In 2009, the government began restructuring its efforts to introduce a nationwide scheme that did not focus on identity cards, but instead the distribution of unique identifiers to every resident, and the implementation of a Centralised Identities Data Repository (CIDR) (Hemant, Srikanth, & Sanjay, 2010). The Unique Identification Authority of India (UIDAI) was established; its responsibility being the implementation, enrolment, and verification of unique identity to the population of India (Unique Identification Authority of India, 2010a).

7.2.3.2 Functionality

UIDAI has claimed to take a very inclusive and pro-poor approach, seeking to ensure that those who are currently locked out of services would be able to prove their identities when required (Unique Identification Authority of India, 2010a). The strategy adopted was that of an online authentication model, where third parties can compare the demographic and biometric information of an individual against the record held in the central database. The UIDAI has issued assurances that third parties will not be able to access or get hold of any personal information held on the CIDR; instead, the UIDAI will only authenticate the accuracy of personal information with a yes/no response (Unique Identification Authority of India, 2010b).

Furthermore, the government has encouraged the use of individuals' unique identifiers as an index within third party systems (Unique Identification Authority of India, 2010b). In several of its use case scenarios, storing and referencing the identifiers has been advocated as a key technique in allowing relevant organisations to monitor the effectiveness of their services, as well as to reduce corruption by tracking employees (Unique Identification Authority of India, 2010c).

7.3 Analysis: Organisational Concerns of Identity

Using grounded theory analysis (Section 5.3.3.2), each of the cases were systematically compared. Viewing identity as a strategic resource, each IDMS was broken down into various underlying processes that aim to maintain or exploit this strategic value. An example of the coding process is governments concern over what identity information to use for verification, with thus affected the identity attributes collected and stored. The underlying factors that influenced these differences were traced, compared, and coded (in this case *authenticity* and *uniqueness* in Section 7.3.1 were the high level constructs identified).

Overall, the analysis revealed that the organisational requirements that affect the implementation and design of an N-IDMS can be divided into two main processes; *identity construction* and *identity use*.

7.3.1 Identity Construction

When an identity system is first implemented, a new and unique context is created, within which several different identities need to be instantiated. It is within this newly created context that an implementing organisation needs to ensure the integrity of all identities within the IDMS. This represents a significant hurdle for the organisation, especially during initial enrolment, as it involves the verification of unknown individuals. When faced with this problem, organisations typically fall back on two main criteria, both of which will have an impact on the overall information that is collected and stored; *authenticity* and *uniqueness*.

7.3.1.1 Authenticity

Authenticity refers to the truthfulness of an identity created within the IDMS. It seeks to answer the question, *is the individual really who he says he is?* Organisations typically ensure *authenticity* of an individual's identity by verifying his/her biographical information (e.g. name, age, address) against various different sources. Consequently, organisations can increase their confidence in the *authenticity* of an identity by placing restrictions on the source of the information, which then affects the list of biographical information that is collected and stored. Organisations can vary the source of information by choosing between two different schemes of identity verification:

1. **Introducer-Based Scheme,** which is built on the concept of personal referrals. It works by having a recognised individual (i.e. a person whom the organisation knows, and believes is trustworthy) vouch for the *authenticity* of another individual who is attempting to enrol into the system.
2. **Document-Based Scheme** that builds on the use of documentary evidence to prove that the enrolling individual is who he says he is. This scheme in effect relies on the third party organisations confirming the *authenticity* of individuals.

While the organisation can vary the identity information, which is stored and used to verify *authenticity*, from either the *introducer or document-based schemes*, it is limited by the context of its implementation; the main contextual factors that influence the applicability of these schemes are:

1. **Universality**
2. **Intimacy**

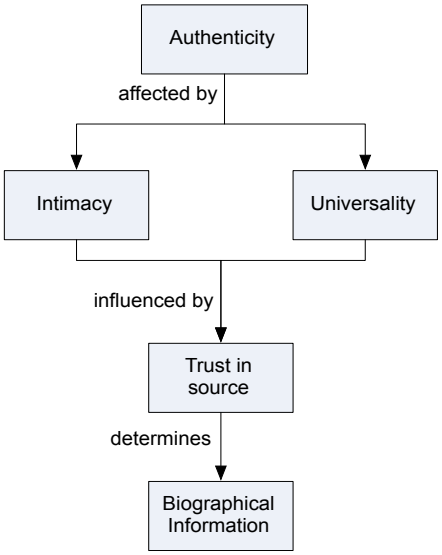


Figure 24 Organisations authenticity requirements

Universality describes the percentage of the target population already possess widely accepted forms of identity documents. These are identities that individuals have typically established with third party organisations, with which they have a trusting relationship (e.g. banks, utilities, and municipalities that have interacted with the individual over a period of time). The degree of *universality* in the targeted population will affect the organisation's ability to rely on a *document-based* scheme to ensure *authenticity*. Specifically, having little to no *universality* would remove such an option from the implementing organisation, as a large number of individuals would not be able to provide the required documents, and therefore would not be enrolled into the new identity system.

The Indian case study provides an example of the implications of low *universality*. In fact, it is one of main issues that the Indian N-IDMS aims to tackle, as low *universality* has direct implications for the individual; in general, low *universality* means that individuals tend to be locked out of both public and private services, as they do not possess any form of recognised identity. This is particularly true for the current poor population in India, where the weak identity infrastructure places unacceptable burdens on the poor population in India.

> *"...every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual. Such duplication of effort and identity silos increases overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes." (Unique Identification Authority of India, 2010a)*

Therefore, India cannot solely rely on a *document-based scheme*, as this would lock out a large section of the targeted population from inclusion in the IDMS. To accommodate for this, the government has shifted the focus towards an *introducer-based scheme, "where introducers authorized by the Registrar, authenticate the identity and address of the resident"* (Unique Identification Authority of India, 2010b).

The UK case study provides a contrast to the Indian context. In the UK, the focus of the identity system lies in the prevention of illegal activities. In all the reviewed documents, the UK government has never mentioned issues about individuals not getting access to services due to lack of identity (it does state that the UK N-IDMS will make it easier to prove identity, but not that individuals are locked out because of a lack of identity). This implies that the UK context already has achieved high levels *of universality*, in that the target population is already in possession of accepted forms of identity.

The UK government took a *document-based* approach, requiring individuals who were to enrol in the system, to provide several different documents as proof of *authenticity* (Blunkett, 2003); i.e. documents that have some form of unique identifier such as passport numbers, driving license numbers, national insurance numbers and *"any number of any designated document which is held by him"* (*Identity Cards Act*, 2006). This information is provided to create an information-net around the claimed identity, which the government can then use to ensure authenticity by verifying the individual's personal information with the relevant third party organisations.

The second factor that influences the choice of a *document or introducer-based* scheme is the *intimacy* that an implementing organisation has with its target population. *Intimacy* captures how much of the targeted population is already known to the organisation. Having high levels of *intimacy* implies that the organisation can be more confident in making use of an *introducer-based scheme*, as it can easily support a transitive trust scheme that extends from known to unknown individuals.

The effects of *intimacy* can be seen in the Bruneian context with its combined approach to ensuring authenticity, incorporating elements of both a *document-based* and *introducer-based scheme*. This is possible because the government has been running an identity system since 1949 (Yunos, 2009). Over that period, the government has been enrolling and storing the identity and personal information of all individuals born and staying within the country, and as a result, has established a great deal of *intimacy* with the general public. Therefore, while individuals are required to provide their birth certificates as documentary proof during enrolment, the government also records the identity numbers of the individual's parents. This in effect creates a hybrid *document-introducer-based scheme* where the authenticity of the individual is proven with a minimal amount of documentary evidence, which is further supported by linkages to introducers that are already enrolled within the system. The advantage for the organisation in using an *introducer-based* approach over the *documents-based scheme* is that is easier to rely on internal systems that they trust, instead of a fragmented approach where different individuals may present different sets of documents to prove *authenticity* (e.g. some individuals may not possess a passport, while others may not possess a driving license).

However, in India, the government's choice of an *introducer-based scheme* was forced by low *universality*. However, India also faces the problem of low *intimacy* to support introducers as it is used in the Brunei case. Having never registered identities of past populations, the Indian government cannot currently rely on parents as introducers to the system. As a result, the government has devised a scheme to artificially boost *intimacy*, by limiting the pool of introducers to a set of trusted recognised introducers. These trusted introducers are required to be registered with, and be recognised by, the registrars that handle enrolment. By making use of such a scheme, the government is more confident of the authenticity of the introducer, and thus the individual being introduced.

While a distinction is made between *introducer-based* and *document-based schemes*, both schemes are not mutually exclusive, in that they both make use of transitive trust to ensure *authenticity* of the claimed identity. The *document-based scheme* is basically an institutionalised version of the *introducer-based scheme*. At the centre of the *document-based scheme* is the implementing organisation's reliance on the documents that have been produced by third party institutions, and can therefore be seen as taking the role of an introducer, as opposed to known individuals in the *introducer-based scheme*. In the end, the *authenticity* of the claimed identity is verified by a third party and the level of trust and confidence the organisation has in that third party.

7.3.1.2 Uniqueness

In addition to *authenticity*, the type of information that the organisation will collect and store is also shaped by the *uniqueness* of an identity. *Uniqueness* refers to the property of an identity not being enrolled more than once into the identity database. Organisations' desire for *uniqueness* is driven by concerns of identity fraud, where individuals might attempt to enrol into the system more than once. A common strategy to preserve uniqueness is through the collection, storage, and use of biometric data.

Today, organisations can choose between various biometrics strategies, with facial, fingerprint, and iris recognition being current solutions of choice. Organisations' choice of biometrics is affected by three main criteria:

1. **Obligations (International standards, Current practices)**
2. **Performance (Accuracy, Human readability)**
3. **Population (Size, compatibility, Geographic diversity)**

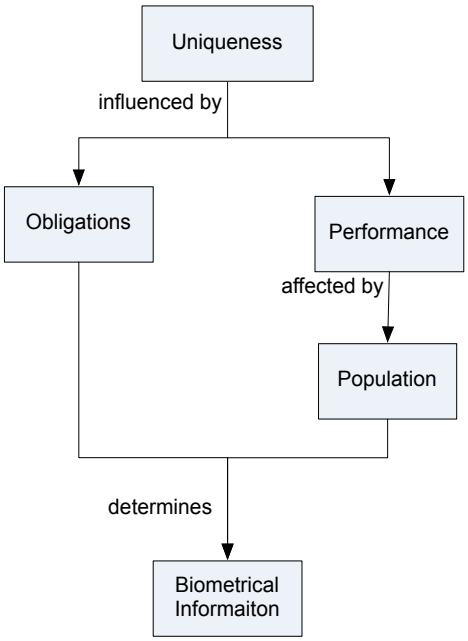


Figure 25 Organisations' uniqueness requirements

The first hurdle that an implementing organisation faces when choosing a suitable biometric technology are the *obligations* that it must conform to. These *obligations* can manifest in the forms of:

1. **International standards**
2. **Current practices**

International standards can have great influence on the choice of biometrics; especially if an individual's identity is meant to be portable across different countries (e.g. travel). In such situations, the organisation aims to achieve interoperability between the different contexts, driving not only the type of biometric to be used, but also the format in which the data is stored. In the UK, the government justified its choice of fingerprints with compliance to international standards published by International Civil Aviation Organisation (ICAO) (Identity and Passport Service, 2006). It should be noted that the actual need for biometrics was greatly debated, as the ICAO standards are only a recommendation, and therefore not compulsory (London School of Economics, 2005); caution should be taken to ensure that *international standards* are not hijacked as an excuse to implement a technology without proper due diligence.

Similarly, although the government of India was not greatly focused on ensuring compatibility with other countries, adhering to an accepted standard would help create a consistent and portable identity within its large borders. As such, the report from the Indian Biometric Committee recommended the implementation of biometrics based on *international standards* (ISO 19794), stating that the *"standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics*" (Unique Identification Authority of India, 2009). *Organisations tend to view compliance to general standards as a form of best practice, irrespective of whether the technology actually supports the overall purpose of the N-IDMS.*

Organisations also face *obligations* around *current practices* that either it, or related third party organisations may have already implemented. The existence of *current practices* around the use of certain biometrics implies the availability of experience, expertise, and infrastructure around that particular biometric. Having such familiarity with a particular biometric can help to ease the implementation of a new identity system that makes use of the same biometric. In the UK context, this can be seen in the relationship between the Identity and Passport Service (IPS) and the Immigration and National Directorate (IND) (Identity and Passport Service, 2006). Prior to the IPS plans to introduce an N-IDMS, the IND had already been processing, recording, and storing facial and fingerprint biometrics of foreigners for the purpose of UK visa applications. Thus, when the IPS finalised its plans for the N-IDMS, it chose to ride on the IND's systems, directly storing fingerprints and facial biometrics on IND databases. In the Bruneian context, the biometrics deployed in the new identity system carried forward practices from the old, making use of fingerprints and facial photographs that they were familiar with.

Aside from *obligations,* organisations are also influenced by the *performance* of the various biometrics; these can be expressed in terms of:

1. **Discriminability**
2. **Human readability**

When implementing a biometric system to ensure *uniqueness*, an organisation will have a confidence threshold that no individual will enrol more than once. This is captured by the *discriminability* of the biometric, which is the performance of the biometric in a one-to-many identification matching process; i.e. comparing an individual's biometric against all other biometrics in the database, thus ensuring that he/she is not already enrolled in the identity system. *Discriminability* of a biometric should also consider the ease of which it can be circumvented. For example, Facial Biometrics is "*considered a poor biometric for use in de-duplication*" as an individual can easily avoid identification through *"the use of a disguise, which will cause False Negatives in a screening application"* (Unique Identification Authority of India, 2009).

Performance should also take into account the *human readability* of the biometric. While the use of biometrics to ensure uniqueness is typically an automated process, a manual form of checking identity is typically required when a false rejection is encountered. Since the system is unable to accurately distinguish between two or more biometrics, human intervention is required to confirm or deny the false rejection. Therefore, having a biometric that enables quick manual forms of checking becomes a necessity. Most biometrics do not lend themselves easily to manual inspection. As a result, despite its low levels of accuracy, facial biometrics become *invaluable* to organisations for the purposes of *human visual inspection* (Unique Identification Authority of India, 2009).

> *"We use AFIS, Automated Fingerprint Identification System. All the fingerprints captured will be processed with the fingerprint matching, and this is very useful when the citizen does registration of the card. This is to ensure that one citizen holds one card and number only. Those who register will go through the AFIS matching, and if it is OK, then we will do the registration. Otherwise there will be human intervention; a matching process, the system will list the possible candidates that match, but normally we go for a 100% match. There is a possibility of 70, 80, 90 and 100% match by fingerprints. The system also makes use of facial image, from the entries identified by AFIS. So it's easy for us to do the matching, we can even assign the matching tasks to the clerk, by looking at the facial image and the percentage. It is very straight forward and user friendly." (Interview with BruNIR)*

The organisation's *performance* considerations are in turn mediated by the *population*, which can affect the *performance* of a biometric in two ways:

1. **Size**
2. **Compatibility**
3. **Geographic Diversity**

First of all, organisations need to consider the *size* of the targeted population. *Large population sizes* can negatively affect the overall accuracy of the biometric. This is particularly indicative in the choice of the ten finger biometrics as proposed in the UK and Indian scheme. The Indian Biometric committee (Unique Identification Authority of India, 2009) established that *"False Acceptance Rate is linearly proportional to gallery size"; u*sing a two fingerprint scheme with a population size of 1.2 billion, the FAR was estimated to be 14%, which is well above the 1% mark that they required. Therefore, the recommendation was to proceed with a ten-fingerprint scheme which was estimated to provide a 0% FAR, maintaining the uniqueness of individuals in the database.

The second *population* characteristic is that of *compatibility*, which captures the suitability of the biometric for use on the targeted population. *Compatibility* can be expressed in two different ways, the most obvious of which is the availability of tests demonstrating that *performance* is not affected by characteristics of the target population (e.g. skin tone, etc.); the lack of such studies was highlighted by the Indian Biometric committee (Unique Identification Authority of India, 2009). Additionally, *compatibility* can also be affected by real world factors. Again, the Indian Biometric Committee pointed to the use of *Lawsonia Inermis* (Henna) by women on the Indian sub-continent, stating that it can prevent the accurate collection of fingerprints as *"sensors may not properly capture fingerprint features."* Another example is the large percentage of population in India who are *"employed in manual labour*", and thus provide *"poor biometric samples",* as their fingerprints have been worn away by the nature of their work. On the other hand, iris biometric is believed to be more compatible with the general population (Unique Identification Authority of India, 2009). Similarly in Brunei, the BruNIR has encountered problems with the compatibility of fingerprints:

> *"... only one, the taking of the fingerprint. Because they can get worn out, and those are very difficult to capture. We identified that since the beginning of the project, and we came up with a solution to make use of moisturizer. It helps, but that is the major problem." (Interview with BruNIR)*

Lastly, *geographic diversity* deals with the spread of the population across space. Large *geographic diversity* can introduce inconsistencies into the procedures, and the conditions under which the data will be collected. When a population is spread across large spaces, the implementing organisation is unlikely to be able to collect all the information on its own; it will probably adopt an accredited enrolment strategy, where authorised third parties collect information on their behalf. UK and India are prime examples of such a situation, where third parties are drawn into the fold, allowing private organisations to enrol and capture individual biometrics, which are then sent to the government's central database. This can result in *"several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts"*, such as the lack of adherence to operational quality, and the differing environmental conditions that affect performance (e.g. face recognition is very sensitive to light changes) (Unique Identification Authority of India, 2009).

7.3.2 Identity Use

In addition to the *information creation* process, the implementing organisation is also concerned about establishing and defining the mechanism in which enrolled identities will be used. In this way, viewing identities as sensitive strategic information that is necessary to carry out various organisational tasks will help to inform the design of the system. By identifying and defining the *purpose* of the identity, the implementing organisation is answering the questions that relate to *"who, what, why and when",* that in turn will help to define the connectivity and overall information access policies. There are four main dependent constructs that organisations focus on when defining the information access policies and mechanisms:

1. **Relying Parties (Organisation, Individual)**
2. **Objectives (Enablement, Proof)**
3. **Conditions (Risk level, Timeliness)**
4. **Accessibility (Information set, Locality, Direction)**

7.3.2.1 Relying parties

At the most basic level, organisations must specify the various relying parties that need to use or access identities on the system; there are two main types of *relying parties (RP)*:

1. **Organisational**
2. **Individual**

First of all, there are the *organisational* entities that need access to the identity, which can further be differentiated into *intra-organisational* versus *inter-organisational* dependence on identity. *Intra-organisational* access of identity is typically a requirement since the implementing organisation needs to create and manage identities in the first place. However, the access of identities within the organisation can extend to support any other functions that the implementing organisation needs to carry out. For example, BruNIR in Brunei is not only responsible for the distribution of the identity cards in the country, but also for the monitoring of identities across the borders. Recent developments have meant that the Brunei identity card can now be used as a passport at land boarders with Malaysia (Sabah and Sarawak). Therefore, BruNIR requires other forms of internal access to support these activities.

This is not the case in the Indian context, where the UIDAI was set up solely to handle the registration of identities, leading to fewer *intra-organisational* requirements. As such, India's main focus lies on the *inter-organisational* access of identity. In its plans to introduce the identity system the UIDAI clearly established and discussed plans with several different third party organisations that include PDS, NREGS, as well as the general education and health provision systems. Meanwhile, the IPS in the UK has defined both *intra-organisational* use of its systems (Identity cards as passports) as well as its *inter-organisational* aims by identifying various agencies that include the Department of Work and Pensions (DWP), the CRB, and law enforcement agencies, among others. The Bruneian context on the other hand has comparatively ill-defined *inter-organisational* obligations, only stating its intention to create a multipurpose smart card that can be used by any third party organisation as necessary.

In addition to the *organisational* reliance on identity, the implementing organisation also needs to recognise the *individual* as an RP that may be able access their own identity and personal information. This is especially the case in the UK scenario, where the IPS has specified that individuals were to able to access all their information on the system, which is envisioned to eventually be an online service (Identity and Passport Service, 2006, 2008, 2009); India and Brunei have not specified any mechanisms by which individuals can directly access or view their identity records, but still have procedures in place that allow an individual to submit information to the implementing organisation after registration.

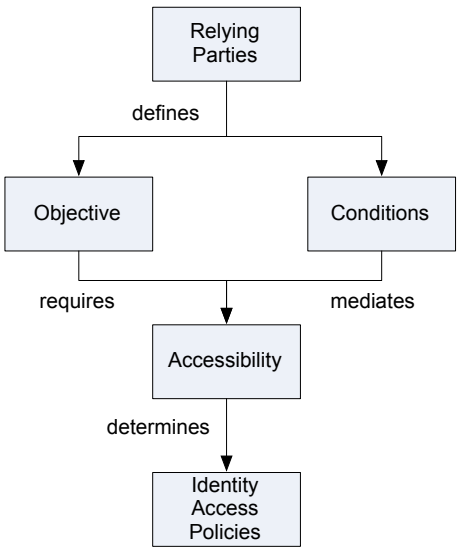


Figure 26 Organisations requirements for identity use

7.3.2.2 Objectives

Each *RP* that the implementing organisation identifies will have its own separate set of *objectives*. These can be expressed in terms of:

1. **Enablement**
2. **Proof**

The use of identity to mediate the provision of services will always create a division between those who have access and those who do not; however, there will always be a dominant mode of use and the other will be a side effect. This dominant intention to use identity to either enable or disable individuals is captured by the *enablement* construct. In India, the main intention of the *RP* is dominated by the enablement of poor people, so as to provide them with access to the services to which they are entitled. Additionally, the Indian banks are focused on introducing new forms of mobile banking, thus enabling individuals to access new services that are to be developed. In comparison, the objectives described in the UK context are those of disablement (benefit fraud, crime, illegal immigration, and terrorism). The Bruneian context has described a largely enabling use of identity, with its intention to support the introduction of new on-line services introduced by third parties.

Proof describes the objective of the *RP* in using the IDMS as a simple single-use proof of identity, or as a key that enables the tracking of individuals' across several different interactions or contexts. The Indian case provides an illustration of a *tracking* scenario where all *RPs* are advised to use the UIDAI as a foreign key to their own systems. It even suggests that the identity be used internally by *RPs,* so as to keep track of employees. The Bruneian case makes no such recommendations nor enforces any rules to such *use*, resulting in a mixed approach, where some *RPs* make use of the identifier as an index to their records, while others merely use the identity as a proof or authentication mechanism.

7.3.2.3 Conditions

The organisation will also need to identify the *conditions* under which the *access to the* identity will take place. These *conditions* capture the operating conditions under which a *RP* will need to access the IDMS; this can be expressed as:

1. **Risk Level**
2. **Timeliness**

Risk level is a measure of the security sensitive nature of the information access. Information access that is done under conditions that can affect national security would be classified high risk, and would have different privileges, when compared to a low risk situation that has little implication for the agency, country, or organisation. The importance of risk level in the development of the identity system and the information access policies is most evident in the UK scenario. In its phased roll out of the N-IDMS, the IPS had clearly identified those working in high security environments (airport and airline workers) as targets for early adoption (Identity and Passport Service, 2009). Additionally, while the IPS defined that all access by third parties would be recorded, any access done in relation for the purposes of counter terrorism would take place without consent, and not be recorded (Identity and Passport Service, 2006, 2008, 2009).

The *risk level* in India and Brunei are not as apparent, but the Bruneian Immigration Department has made an official channel by which law enforcement can send in a written request, with sufficient supporting reasoning, to get hold of certain information. Meanwhile, the UIDAI has not specified any direct access to the information by third parties. However, in its plans for the N-IDMS it was pointed out that the unique identifier per individual would be incredibly useful for third parties to keep track of employees that might pose a risk from corruption.

In addition to *risk level*, the *timeliness* of the information access is another factor to consider. Considering that one of the many cited benefits of an identity system is the efficiency gains, it is not surprising that the time pressures of the information access are an important consideration when considering the accessibility to the identity system. An example of this is the use of the UK N-IDMS for the purposes of Criminal Background Checks (CRB) when applying for certain working positions (e.g. work that involves interaction with minors). The problem raised by the current CRB procedure is that it takes a long time for them to confirm individuals' identity, thus leading to a backlog of applications. Therefore, it is imperative that the agency handling these background checks get responses in a more timely manner, and are therefore seen as a prime candidate for gaining some form of access to the identity system; *"the time for issuing Criminal Records Bureau (CRB) disclosures could be reduced from 4 weeks to 3 days"* (Home Office, 2005).

The Indian government has also highlighted the time sensitive nature of third parties, stressing the importance of addressing the application of current ration cards due to "*prolonged delays in processing the application*" and the advantages in using the unique ID number in the distribution of rice grain (Unique Identification Authority of India, 2010d). The Brunei N-IDMS has no specific examples regarding the timeliness of information, but general efficiency was a main factor in the introduction of the smart card system, as it would allow the transfer of information in digital format reducing the overhead for filling in forms (Interview with BruNIR).

7.3.2.4 Accessibility

Once the organisation has identified the *RPs* and their respective objectives, it can then go on to define the *accessibility of the system to these parties*. This access to the system can be described in terms of:

1. **Information set**
2. **Locality**
3. **Direction**

Information set describes the type and amount of identity information that the organisation will need or have access to. In the UK case, with its emphasis on national security and terrorist prevention, the IPS has clearly defined that the authorities would be able to gain access to all the personal information on the database of potential suspects. In India no *RP* will have access to the personal information, but the UIDAI will only confirm or deny the accuracy of personal information held in their database. The immigration services in Brunei has stated that third party organisations will not have any access to the database, and can only access the information that is visible on the card and stored on the smart chip.

Locality refers to the spatial mode of access to the identity system. On the one end, *locality* of access can be confined to the physical location where the identity is presented to an individual. The other extreme lies with the remote access of identity through a networked database. The Bruneian N-IDMS does not provide third parties with any remote access to their database; all the information and authentication functions that the relying party can access are stored on the card itself. This is in contrast to the Indian N-IDMS that emphasises remote authentication procedures, where the UIDAI would communicate with third parties across a network. The UK N-IDMS has specified a range of access options that include local options such as visual authentication and local chip authentication, but also specifies methods that allow fingerprint authentication across a network, to match records in its database.

The *direction* of the information access is another dimension that the implementing organisation needs to consider when providing third parties privileges to the identity system. *Direction* captures the push or pull nature of the identity access, which in turn defines the readability (including authentication procedures) or write-ability rights of the third party. On the one hand, the Indian N-IDMS does not provide relying parties with any privileges to write information to the database. The transactions are primarily a pull of information, where the third party requests authentication of identity. On the other hand, the UK N-IDMS also records information about the third party access when performing authentication procedures. A new entry is created on the database recording the time and location of the authentication; this represents a combined push and pull operation, where information is sent and stored on the identity database. Meanwhile, the Bruneian N-IDMS does not provide any remote access, but certain third parties (law enforcement) can still make queries through written means, which is a remote pull of information. However, third parties can also store information onto the chip when required. This represents a local push of information onto the card, and therefore affects the overall information access policies that need to be provided.

7.4 Ensuring "Fit-for-purpose"

Finally, while the previous sections have outlined the organisation's concerns over the construction and use of identity, it is the *purpose* of the system that drives these requirements. Who are the relying parties that require access, and what identity information does the system need to hold? These questions are answered through a definition of the *purpose*, which then informs the organisation's *identity construction* and *use* requirements, striving to ensure that the system being implemented will be fit for its purpose.

Take India for example, with a defined *purpose* to enable the poor to gain access to services, was quick to identify welfare organisations as relying parties, while also ensuring that individuals' are able to enrol by devising the appropriate authenticity requirements for a target population that suffers from both low universality and intimacy. Similarly, the UK, with the focus of the purpose resting on the reduction of crime and terrorism, was able readily to identify law enforcement agencies as a core relying party, as well as defining strict authenticity and uniqueness requirements that would support its security goals.

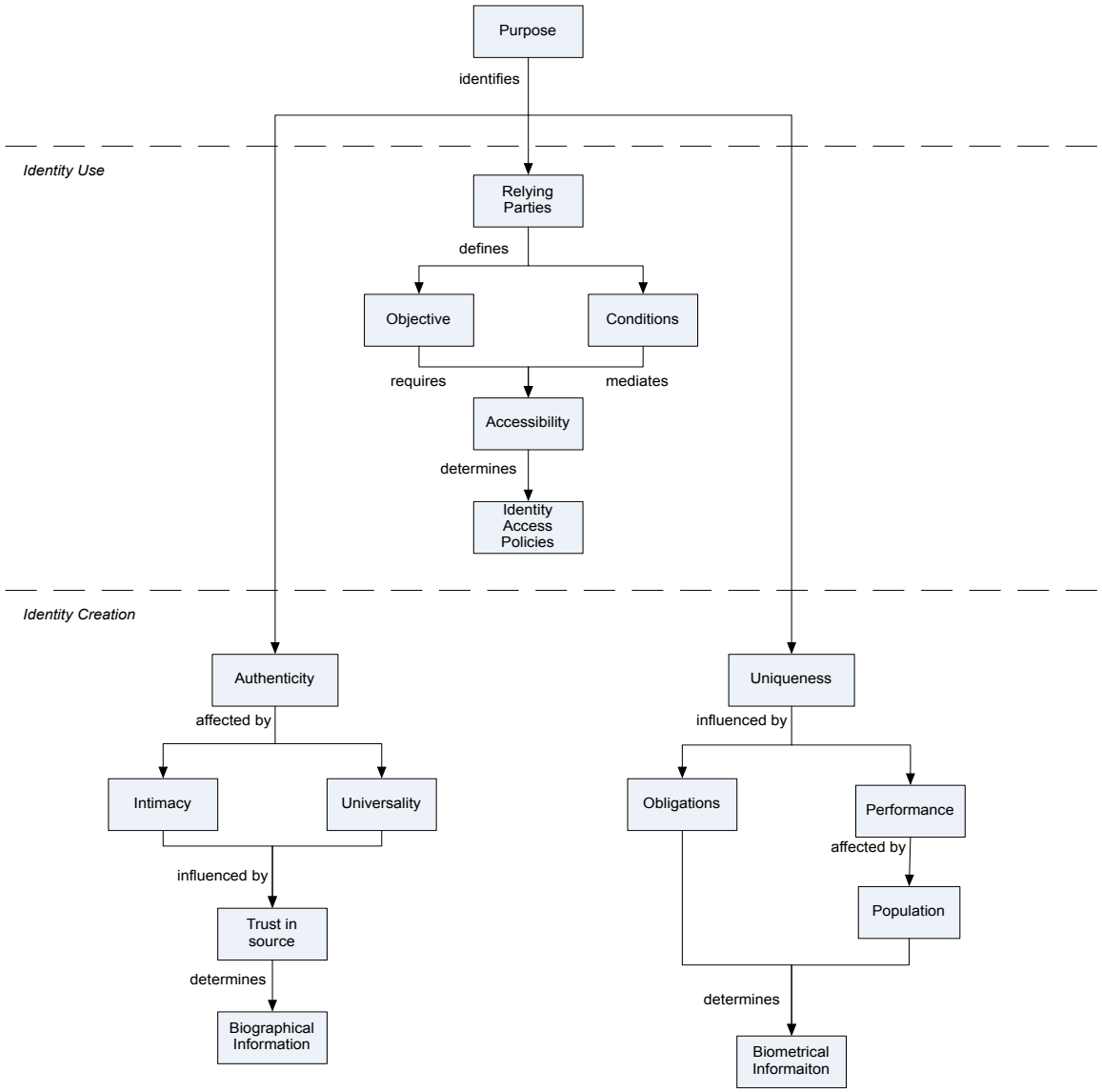


Figure 27 Framework of organisations identity requirements and how it affects design

7.5 Summary and Discussion

A case study approach was used to explore organisational concerns and requirements when implementing IDMS; specifically, the focus of research was on government implementation of N-IDMSs. Using a case study approach, research focused on systems implemented in three different countries; Brunei, India and Britain. Grounded theory analysis was used to analyse the documents and interviews collected from each case study.

Overall, the analysis showed that the *purpose* of the system drives the organisation's identity requirements, and thus informs its two main concerns when implementing IDMSs:

1. **Identity Creation** that is concerned with the enrolment process, and the correctness of the identity instantiated within the system.
    a. **Authenticity** deals with the truthfulness of an individual's identity. Ensured by collecting and verifying various biographical details. Organisations can collect biographical information using a document-based or introducer-based approach; this choice is affected by:
        i. **Universality** is percentage of the target population that already possesses widely accepted forms of official identity that the organisation can then verify against third parties.
        ii. **Intimacy** captures how much of the targeted population is already known to the implementing organisation, and can thus vouch for the individual.
    b. **Uniqueness** ensures that an individual does not enrol within a system more than once. This can be done through the use of biometrical information; the organisation's choice of biometric is affected by:
        i. **Obligations** are current requirements that an organisation has to implement or consider, such as pressure from international standards (international obligations, current practices).
        ii. **Performance** defines the accuracy of the biometric in producing matches (accuracy, human readability).
        iii. **Population** describes the real world human factors that can affect the performance of the biometric (size, compatibility, geographic diversity).
2. **Identity** use is concerned with the process of establishing and defining the mechanism that enables relying parties to access and use identities in the system.
    a. **Purpose** describes the situation or problem that the IDMS is meant to support.
    b. **Relying Parties** are the various users and third parties that need access to the identity to complete a task (intra-organisation, inter-organisation, individual).
    c. **Objectives** detail the relying parties' intention and requirements to use the identity (enablement, proof).

d. **Conditions** capture the situational factors under which the relying parties operate (risk level, timeliness).
e. **Accessibility** describes the manner in which the organisation will access the identity (information set, locality, direction).

The findings of this study overlaps and further the current recommendations in the field; the codification of the identity requirements into a framework can be used to further aid discussions and critiques of IDMSs. For example, Kent & Millett (2002) state that attention should be paid to issues of purpose, population scope, data scope, and users of the data. The concerns are all addressed in the framework in more specific details, while also exposing the relationships between the various considerations. Similarly, Whitley & Hosein, (2010) describe a short-circuiting of identity debates through the use of international obligations, language ambiguity, technological focus, and expertise. The framework addresses these concerns by explicitly listing the considerations, thus reducing ambiguity, while also highlighting non-technological decisions such as *relying parties*, and their unique *objectives*.

The *uniqueness* component of the framework provides another area of comparisons to available work in the field. The focus here lies in the biometric technology and considerations, which is an area drawing much attention. Drawing from Ashbourn's (2000) recommendations for implementing biometric systems, organisations should not only pay attention to the False Acceptance and Rejection rates, but also outline population considerations such as ease of use; these are all present in the framework as sub-dimensions of the *performance* and *population* constructs.

7.5.1 Future Work

A limitation of the current research is its emphasis on biometric systems; this is due to the three different systems chosen for investigation falling under the similar design patterns. However, even without biometric systems, *uniqueness* is still an important trait, and will then fall onto other authentication mechanisms. Future work will need to address these concerns and further develop the framework to be applicable to non-biometric implementations.

Work will also need to be done to develop guidelines to effectively express requirements for *uniqueness, authenticity* and *purpose*; doing so will further help to increase communication in the field and encourage adoption of the framework, this ensuring that IDMSs implemented will be fit-for-purpose.

Chapter 8: Unified Framework to Human-Centred Identity

This chapter brings together the findings from the system, individual, and organisation studies, synthesising a unified framework that provides a holistic view for a human-centred IDMS.

A result of the research here shows that the organisational identity requirements guides the design and implementation of an IDMS, and thus affects the individuals lived experience; the *identity creation* process, influenced by the organisation's *authenticity* and *uniqueness* requirements, will have an impact on the *metrical properties* of the system design (Section 8.3.1); while the *identity use* process which determines the *information access policies* will determine the *structural properties* of the IDMS, dictating the flow of the information within the system (Section 8.3.2).

Additionally, the *system design* in turn has an influence on individuals' perceptions of identity. The *metrical properties* affect individuals' *system judgement*, working through their perception of *information quality* (Section 8.4.1). The *metrical properties* combined with the *structural properties* influence the individuals' *security concerns* (Section 8.4.2).

8.1 Drawing Research Studies Together

This chapter provides a holistic view for a human-centred approach to IDMSs, that takes a multi-stakeholder approach that covers the organisations' identity requirements, individuals' perception of identity systems, as well as the impact of system design on the lived experience of the individual; it ties together the findings obtained from the previous studies detailed in this thesis (Chapter 5, Chapter 6, and Chapter 7), resulting in a unified framework that details the various processes and interactions that take place within the development, implementation, and use of an IDMS.

The unified framework presents an integrated narrative of the identity ecosystem, providing practitioners and researchers with an in-depth understanding of how each element interacts and influences the others.

8.2 Methodology: Developing a Unified framework

In analysing the available literature in the field, this thesis puts forward the argument that current approaches, such as privacy and trust, are insufficient to developing human centred solutions to national identity systems (Section 3.2 and 3.3). In doing so, an outcome of the literature review was the identification of three different perspectives that are central to understanding IDMSs (Section 3.4)

1. **System**
2. **Individual**
3. **Organisation**

These perspectives formed the basis of three separate studies, each designed to analyse the human aspects that shape and define the development of IDMS. A result of each study was a framework that detailed the various constructs and relationships that shapes the development and implementation of an identity system.

The system study resulted in a system design framework that accounted for the lived experience of identity (Chapter 5). The framework consists of two broad sets of system properties that explain how the design of an IDMS affects the everyday lives of individuals that are enrolled into the system:

1. **Metrical Properties**
2. **Structural Properties**

On the other hand, the individual study (Chapter 6) sought to identify how individuals develop initial intentions to accept IDMS. This resulted in a framework that outlines individuals' perceptions and concerns when faced with a new system. The study identified several main concerns that influence individuals' perceptions:

1. **Situation Perception**
2. **System Judgement**
3. **Security Concerns**

Finally, in contrast to the individual and system studies, the organisation study (Chapter 7) looked at organisations identity requirements that influence the design and implementation of an IDMS. The resulting framework identifies that organisations are focused on the processes of:

1. **Identity Construction**
2. **Identity Use**

Although each framework approaches identity from a different perspective, the results of the three studies are compatible with one another, as the constructs from each framework overlap and influence each other. These influences between each framework identify relationships between the respective frameworks, and thus enable the development of a unified theory and narrative about the design, acceptance, and implications of identity. Furthermore, the overlaps between the different research perspectives also acts as a form of data, method, and theory triangulation (Section 4.44.4), thus boosting the robustness of the research, extending the validity and reliability of the findings.

Applying the grounded theory approach that underlies the overall research, this thesis went back to re-analyse all the qualitative material gathered from each of the studies; the analysis here differs since it brings forward the theoretical constructs developed throughout this thesis. Using a basic timeline structure, the analysis focused on exploring relationships and causality between the frameworks. At an initial stage, the implementation of an IDMS is triggered by a problem the organisation wants to address; the organisation assesses the situation and designs an IDMS to support their activities in addressing the issue. The proposed design then affects individuals' perceptions and acceptance of the IDMS. Finally, over time the true impact of the identity system design on the lived experience, as separate from the initial perceptions, emerges.

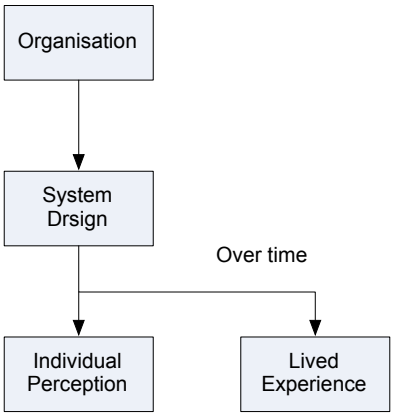


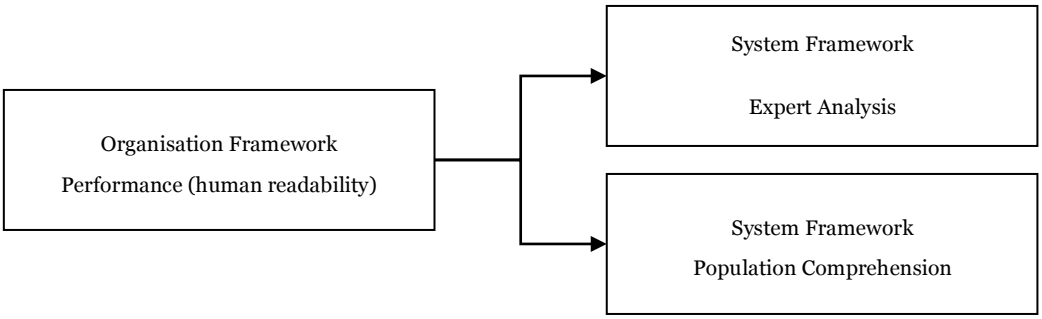
Figure 28 Basic interactions between the organisation, individual, and system framework

8.3 Organisational Requirements to System Design

An implementing organisation is typically a prerequisite to building an officially recognised and accepted identity system. An organisation introduces a system to aid a specific purpose; therefore, from a high level view, it is straightforward to identify that the organisation identity requirements will inform the system design. By inspecting these two frameworks, we can identify in greater detail the relationships between the organisation framework and the system design framework.

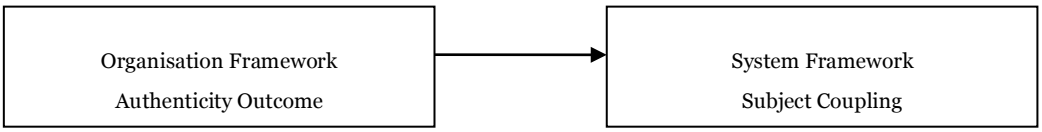
8.3.1 The Process of Creation and the Capturing of Identity

As identified in Chapter 5, the system design has two major sets of properties; structural and metrical properties. The metrical properties deal with the type of information that makes up the identity within the system. Recall that in developing the system, the government is concerned about the creation of identity, aiming to ensure the authenticity and uniqueness of all individuals enrolled into the system. These concerns will affect the final set of biographical and biometric data, and therefore feed directly into the metrical properties of the system design.



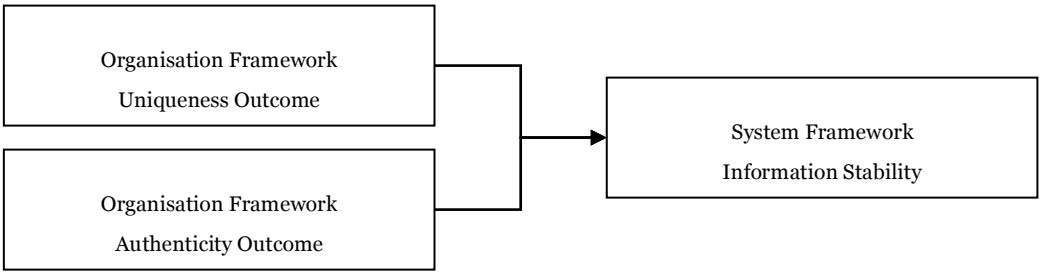
Expert analysis is driven by the final choice of *biometrics*; the more technical or specialised the information collected is, the more specialised training and knowledge is required to interpret the information. This is linked to *population comprehension*, as individuals are typically unaware of the way in which biometric processes work. Therefore, the level of *expert analysis* and *population comprehension* is an outcome of the *uniqueness* requirements; the *human readability* concern is of particular importance. *Human readability* allows for human intervention in the analysis of the identity attribute; the biometric (e.g. facial photograph) is easily deciphered or read by a person. Therefore, emphasising *human readability* lowers *expert analysis*, while at the same time increasing *population comprehension*.

For example, in an enrolment proof of concept study conducted in India, individuals were *"often confused"* on what they need to do when introduced to the iris biometric (Bannur, 2010).



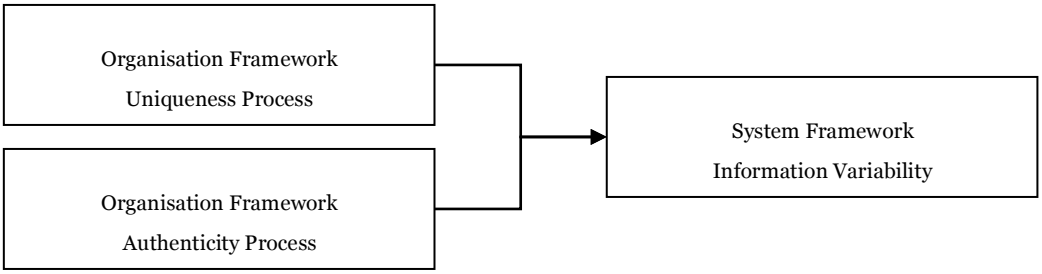
On the other hand, *subject coupling* is influenced by the *authenticity* requirements of the organisation. *Subject coupling* is concerned with the matching of the identity instantiation to the relevant partial identity. This largely deals with the biographical attributes of an identity, where collecting too much or too little information reduces *subject coupling*. Therefore, *subject coupling* is influenced by the *authenticity* process, which determines the final set of biographical details that are required. Requesting a large number of documents or requiring too many individuals may reduce *subject coupling* as it increases the risk of collecting information that may be seen as irrelevant to the context in which the implementing organisation operates.

In reference to the UK N-IDMS intention to support travel functions, the report from the London School of Economics (2005) states that the *"UK proposal would call for further evidence or information that would appear to be contrary to the spirit of the Directive."* Furthermore, the report states *"it is difficult to see how the requirement for all this information can satisfy the 3rd Data Protection Principle by being relevant, adequate, and not excessive for the proposed purposes."*



Meanwhile, *information stability* is influenced by both the *authenticity* and *uniqueness* outcomes. The biometrics chosen as part of the uniqueness process typically have a certain lifespan that lends itself to the stability of the identity instantiation; *"In the case of facial recognition, it would seem advisable to update the templates at least every 10 years. Fingerprints and iris should be considerably more stable*" (Home Office, 2005). Additionally, the biographical information chosen as part of the *authenticity* requirements can also change and vary with time (name, address, marital status, etc.), thus affecting the stability of the identity.

In relation to updating address details stored in the Brunei N-IDMS, the BruNIR commented that *"some people don't even do that"* (Interview with BruNIR). This is further supported by interviews with the LTD stating that authorities tend to refer to the information stored on the LTD database, as *"it is renewed more often"* (Interview with LTD).



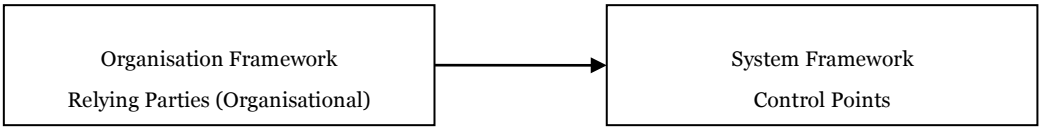
Like *subject coupling*, *information variability* is influenced by both *authenticity* and *uniqueness*. A *document-based authenticity* scheme can result in the collection of information across various contexts that can then be pieced together to form a complete identity, allowing new inferences about an individual to be made. Similarly, an *introducer-based scheme* that relies on a large number of introducers will mean that the organisations are able to tie various individuals together, thus creating an opportunity to build on the individual's social circle. In both these situations, the *information variability* is increased, as the *authenticity* process requires a large number of documents or introducers.

The LSE report on the UK N-IDMS (London School of Economics, 2005) raises these concerns on the potential ease with which various databases can be *"combined to provide the government with a comprehensive and all pervasive database on the lives of its citizens."* The Brunei and India case studies also raise similar issues because of the ubiquitous use of unique identity numbers across various contexts.

Information variability is also influenced by the biometric chosen, and therefore the organisation's *uniqueness* requirements. Although this relationship is not as clearly defined as the impact of the authenticity process, different biometrics lend themselves more readily to other uses, and therefore may increase the level of *information variability* in the process.

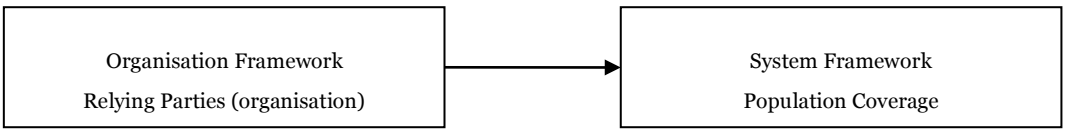
8.3.2 Using Identity and the Flow of Information

While the *identity creation* and maintenance process informs the *metrical properties* of system design, *identity application* determines the *structural properties* of the system. The identity application process revolves around the use and accessibility of the identity by the various relying parties; this is intimately tied up with the structural properties that focus on the flow of identity information within the identity ecosystem.



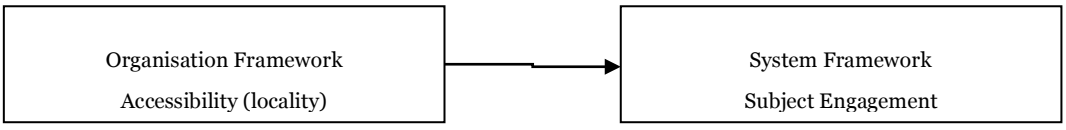
First of all, there is the influence that *relying parties* have on the *number of control points*. In designing and planning the various uses of the identity system, the organisation needs to identify all the third party organisations that require access to the system. Thus this can shape the *number of control points* present; the more *relying parties* identified, the higher will be the *number of control points*.

The Indian government identified several different *relying parties* pre-implementation (PDS, Education Agencies, Public Health Agencies, MGNREGA, as well as working with banks to facilitate micro-payments). The UK government has identified various *relying parties* that span private and public bodies. The Brunei government did not identify any specific *relying parties* when upgrading its identity system, but carried forward practices where public and private agencies rely on the identity number to identify individuals. Thus, every time the identity is required, it adds to the overall *number of control points*.

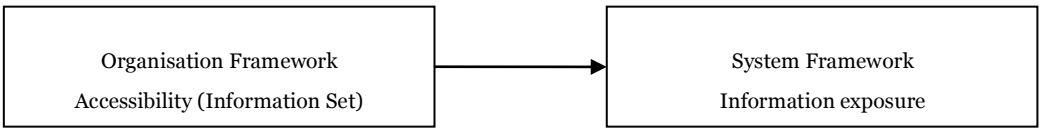


The *relying parties* also have an indirect implication on *population coverage*. Each *relying party* that needs access to the data is likely to be targeting specific portions of the population. Therefore, the greater the number of *relying parties*, the greater the targeted population will be. Hence, *population coverage* would increase along with the number of *relying parties* identified.

When planning the UK N-IMDS the IPS had plans to change the system from being a voluntary to compulsory status, thus enabling all organisations to become third parties, which then makes the identity card the de facto proof of identity in all situations (Blunkett, 2003).



Another relationship is the effect of the accessibility degree of *subject engagement*. *Subject engagement* is influenced by how active or aware an individual is in the use of his/her identity. Therefore, systems that have defined remote accessibility options for third parties will lower the *subject engagement*. In contrast, IDMSs that only specify local access to the identity (e.g. through the use of a card), will have a high level of *subject engagement*.



The use of identity also has an impact on *identity exposure*; it is affected by the identity information accessed by a *relying party*. A *relying party* that has access to a large amount of information will increase the risk of information exposure, while relying parties not having access to context information will decrease the risk or effects of exposure.

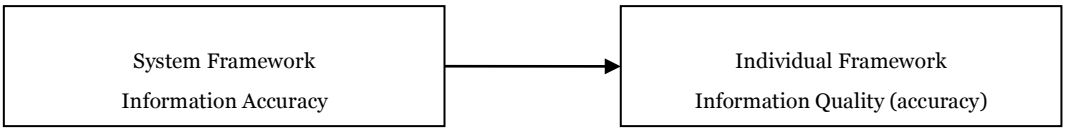
In highlighting the lack of proper controls after an individual's information is obtained, the LSE report (London School of Economics, 2005) states that it could have *"a devastating impact on those who have good reasons for avoiding the existence of easy means of identification. This would include, for example, those in senior government or military positions who may be terrorist targets, those who might be subject to harassment or attack from 'animal rights' activists or from other extremist groups. Those who wish to hide from stalkers or from those who wish to harm them will also be at increased risk."* The Indian N-IDMS does not release personal information to any relying parties, and therefore does not suffer from the same issue.

8.4 System Design to Citizen Perception

While the *organisational requirements* eventually lead to the *system design*, it is the *system design* that will influence *individuals' initial perceptions*. However, this needs to be differentiated from the *lived experience* of the system, since the system has not yet been operational. Following the individual perception framework (Chapter 6), an individual develops his/her perception of the acceptability of an identity system based on considerations of certain aspects of the identity system. Therefore, by analysing the individual perception framework and the system design framework together, a relationship may be established whereby the system design properties have an influence on the development of an individual's perception of the IDMS.

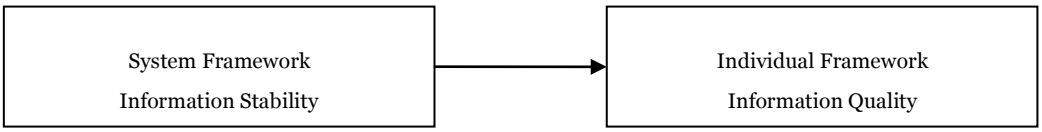
8.4.1 Informing System Judgement

At an initial level, the strongest and most identifiable relationship between *system design* and *individual perception* takes place around the individual's *system judgement*. *System judgement* is developed through an assessment of the various types of information, how it is collected and used. These are exactly the issues that the system design properties are designed to tackle; *metrical properties* deal with the type of information, while *structural properties* deal with the flow of information. In recognising these similarities, a map of influences can be developed, linking a specific design property to a particular area of individual assessment.



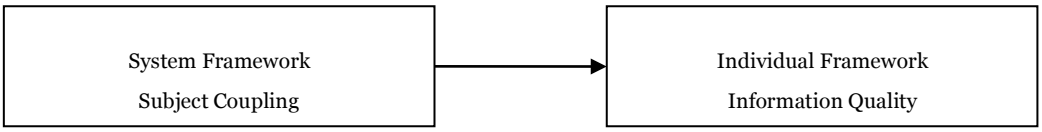
Information accuracy has a direct impact on an individual's perception of *information quality*; low *information accuracy* will negatively affect perceptions of *information quality*. Focus group participants were quick to point out inaccuracies in the information collection processes, and were concerned about the usefulness of the information on the system to information organisational decisions.

In the discussion of *Scenario 1 (child abuse),* focus group participants were vocal about the quality of the notes made by carers regarding their suspicions of abuse. From their perspective, the notes had a high chance of being inaccurate, as most carers would be quick to attribute any injury to abuse.



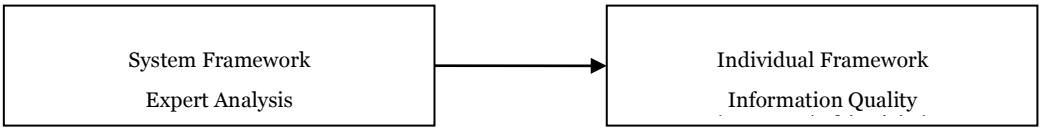
Perception of *information quality* is also influenced by *identity stability* of the system; specifically, *identity stability* may have an effect on the individual's perception of *completeness*. Based on the individual perception framework, individuals may have concerns on the ability of the system to collect all the intended information; not being able to do so creates an inaccurate portrayal of the individual, thus reducing accuracy. From the focus groups, participants readily identify issues with completeness in situations where information is constantly changing, as the identity system might not be able to cope with the frequency of change. These concerns are captured by the *identity stability* design property; identities that change frequently have low stability, while identities that are constant over time have a high level of stability. Therefore, a high level of *identity stability* has a positive impact on an individual's perceived *information accuracy*.

Focus groups regularly raised issues of completeness in *Scenarios 2 (personal debt) and 3 (obesity)*, where new information was constantly generated; the system would not be able to capture all the new information that was being generated.



Another relationship is that of *subject coupling* to *information relevance*. Recall that *subject coupling* deals with how well the identity instantiated within the system matches on to the partial identity within its context of use; collecting too much or too little information can create an un-representative identity. This matches the individuals concerns around the issue of *information relevance*, where too much or too little information may be indicative of the *granularity* of the information collected. Therefore, as the degree of subject coupling decreases, the individual's perception of relevance will decrease along with it.

For example, in discussing *Scenario 2 (personal debt)*, focus group participants were typically concerned about the collection of specific information on single item purchases, stating that identity created does not match the role of the individual to the organisation. *"Yeah, the government pulls information from all stores about purchasing habits, I don't think what you buy is relevant in the least, as long as you are repaying. It is more about your bank accounts, then what you are actually buying, that is just not relevant" (Focus Group 5,Brtisih, Scenario 2).*

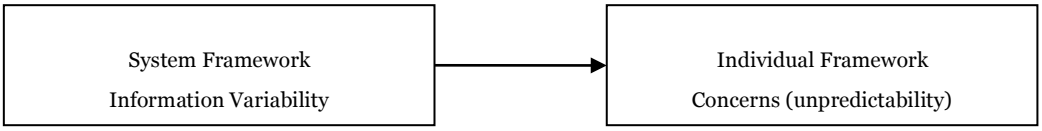


Another identifiable relationship is that of *expert analysis* to *information accuracy*. From the individual study, individuals are highly concerned with the *subjectivity* of the information that is being collected and used; the individual perceives this information as being inaccurate. The *expert analysis* metrical property describes the amount of human intervention required to process any identity information, thus capturing the subjectivity vs. objectivity dimension of the identity. Therefore, the degree of *expert analysis* should have an impact on the perception of *information accuracy*. The lower the degree of *expert analysis*, the more objective the identity process is, and therefore the higher will be the perceived *information accuracy*.

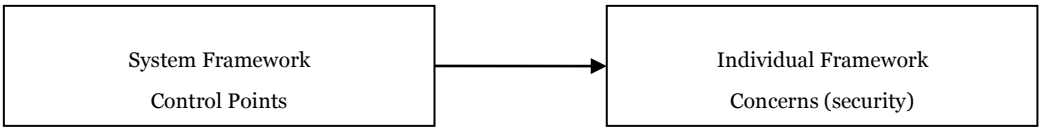
In the analysis of the UK DNA database scheme, experts raised issues of accuracy regarding the DNA matches; especially those with samples from crime scenes, which may be contaminated, thus requiring human interpretation of the results. Focus group participants also raised similar concerns regarding the accuracy of the DNA interpretations, as well as the data collection procedures that required interpretation from *experts* such as doctors and teachers in *Scenario 1 (child safety)* or employers in *Scenario 2 (benefit fraud)*; a typical suggestion was to reduce the level of interpretation by creating numerical weights on certain criteria, thus creating a more objective process.

8.4.2 Fuelling Concerns

Aside from *system judgement*, development of the overall perception is also influenced by an individual's concerns about the information within the identity system. These concerns appear in the form of general security breaches and information leakage, as well as the future unpredictability in how the information might be used. Again, these issues stem from the design of the IDMS, indicating a relationship between system design framework and individual perception framework.

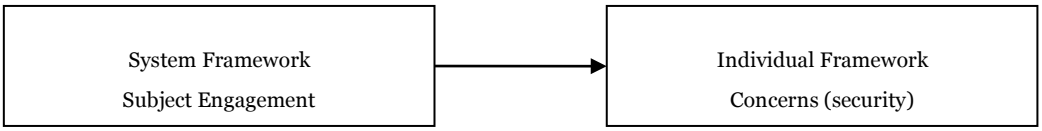


Dealing first with the issue of *future unpredictability*, these concerns are typically raised when individuals do not have confidence in the implementing organisation to restrict the use of the identities to the originally specified purpose. The type of information being collected influences these concerns. Specifically, systems with high *information variability* are those in which the identity lends itself to use beyond its original context. Therefore, IDMS with high *information variability* would raise concerns about *future unpredictability*, while low *information variability* would serve to reduce such concerns.



Number of control points may also play a part in shaping an individual's *concerns* around the security of the system. The individual study revealed that individuals had concerns about the abuse of information by *insiders*, as well as the access of information by unauthorised individuals. From a system design perspective, the *number of control points* expresses the frequency of access to that information.

During the focus groups, participants commonly suggested that access to the information be controlled by reducing any access to situations that require them, thus preventing possible abuse. This in effect reduces the *number of control points*, thus potentially reducing an individual's concerns around security.



Finally, *subject engagement* also drives individuals' concerns. Focus groups participants were constantly wary of situations in which their information is constantly accessed without their involvement. Systems with a low *subject engagement* are seen to be more open to *abuse* and information leakage, as the individuals' believe that they have no control over how it is used. This creates situations of uneasiness, which fuels their concerns.

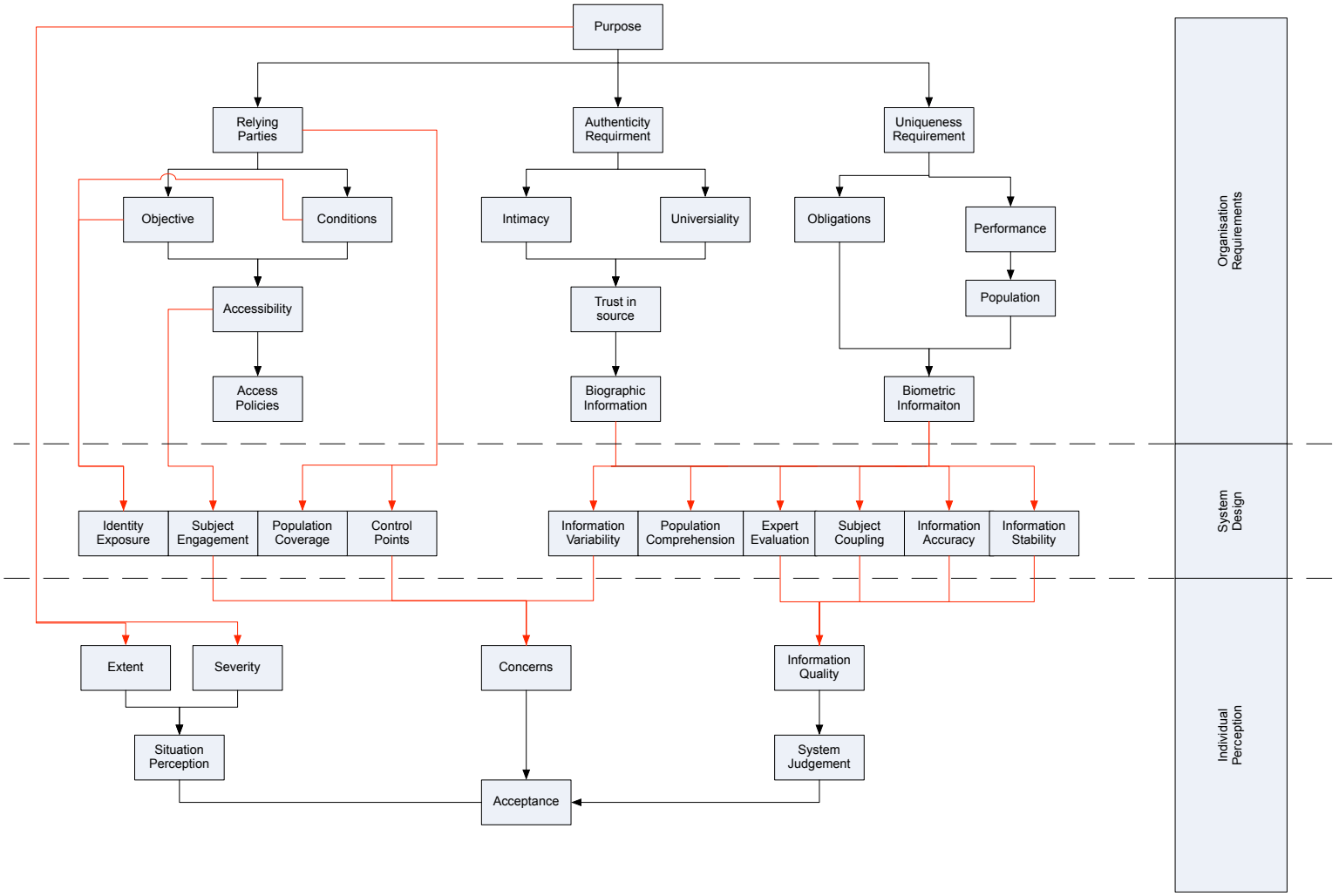


Figure 29 Unified Human-Centred Framework

8.5 Discussion and Summary

In undertaking research into a human-centred approach to identity management systems, this thesis approached the subject from three different perspectives; the system, the individual, and the organisation. Separate studies were designed around each perspective, resulting in the development of three different frameworks that detail their respective issues.

The research here moved on to synthesising a unified framework of the phenomenon, beginning from organisational requirements that inform the system design, and which in turn have implications for individual perception and acceptance. Continuing on with a grounded theory approach that underlies the three different studies, research went back to re-analyse all the available material, bringing along with it all the theoretical concepts identified in each previous study. This resulted in the discovery of relationships between the different frameworks, where:

1. **Organisational Requirements inform System Design**
    a. Identity Creation requirements determine the metrical properties.
    b. Identity Application requirements determine the structural properties.
2. **System Design inform Individual Acceptance**
    a. Metrical properties influence Judgements (through perception of Information Quality).
    b. Structural and Metrical properties influence Security Concerns.

Tying together the outcomes from the three separate studies in this thesis (i.e. the system, the individual and organisation studies) has resulted in a framework that provides a multi-stakeholder narrative for a human-centric IDMS. Comparing this framework to the available literature reveals similarities present within the identity policy domain. For example, the policy literature has emphasised the importance of finding a purpose, stating that it will have ramifications for the underpinning design of the system (Kent & Millett, 2002; Whitley & Hosein, 2010). This is reflected in the unified framework where purpose forms a key construct that influences organisations authenticity and uniqueness requirements. Furthermore, the unified framework also stresses the importance in working together with Relying Parties and designing identity systems to ensure that their objectives are met; this addresses the shortcomings of current approaches to N-IDMS implementation, that does not account for the multidisciplinary nature of N-IDMS thus leading to a lack of interaction between the organisation and other important stake holders (2010b).

The unified framework, also illustrates the implications of the organisations requirements on the design of the system, and thus its eventual effects on individuals' initial perceptions of the system, as well as the effects on individuals' overall lived experience. Identity policy makers typically reduce "*the societal problem [that the IDMS addresses] to a technical problem*"(Kubicek & Noack, 2010b). However, the unified framework stress the relationship between the organisation, the technical system, and the individual thus helping to address these concerns, encouraging the organisation to think beyond the technical details, and thus focus on the relationship of the purpose, the identity requirements, the design of the system, as well as individual concerns regarding the IDMS.

Finally, while research was done until theoretical saturation, with respect to the research material analysed, there may be other factors or relationships that exist but have yet to be uncovered. For example, there may be other system properties that exist, and thus other potential relationships between the frameworks. That said, given the variety of cases analysed and compared to each study, the factors and relationships in the framework represent key core constructs and relationships that would be applicable to most IDMS.

8.5.1 Future Work

The work here would greatly benefit from further description of the relationships between the various frameworks and constructs. This holds especially true for the relationships between the organisations' *identity creation* requirements, and the *metrical properties* of system design. Currently, the relationship is expressed at a high level, stating that the choice of biographical information will have impact on *subject coupling*, among other factors.

The unified framework would also benefit from the suggested improvements made to each part of the framework (Section 5.4.1, Section 7.6.1, and Section 7.5.1); for example, in Section 7.5.1 the suggestion that future work should aim to develop proper guidelines to express requirements and outcomes would then feed into the unified framework, enabling for finer relationships to be established. Furthermore, the relationships between the different perspectives can be used as a reference point to further develop each perspective; for example, the *authenticity requirements or biographical choices* can be expressed in terms of the *metrical properties*.

Chapter 9: Evaluation of the Framework

This chapter discusses the criteria used to judge the quality of the qualitative research in this thesis, reflecting on how rigor, and by extension validity, is built into the approach taken by this thesis (Section 9.1.1).

A summative evaluation to test the effectiveness of the framework in the design of a real world IDMS implementation is not feasible. Thus, validation of the research findings was done through a formative evaluation of the framework, using expert reviews to assess completeness and usefulness of the framework (Section 9.2). Overall, experts agreed that the constructs and relationships in the framework reflected real world concerns, and proved useful to both researchers and practitioners.

However, experts expressed areas for further improvement, including clarity of terminology, existence of other system design properties and relationships, the need for greater detail of individual perceptions, as well as the addition of an attacker perspective to the framework (Section 9.3).

9.1.1 Evaluation of Research

While quantitative strands of research have standard measures of validity (the covariance matrix) and reliability (cronbach alpha), qualitative research does not; indeed the non-numerical nature of the data being analysed does not allow for the calculation of such figures (Corbin & Strauss, 1990). Combined with the variety of data collection and analysis procedures, researchers have put forward various different criteria for evaluating qualitative research (Seale, 1999; Silverman, 2004); *"A review of all the concepts that have been proposed… would be a major enterprise with dubious value"* (Seale, 1999).

Within this diversity of qualitative evaluation criteria, Lincoln & Guba (1985) provide a basis for the most influential work. In their work, they detailed 4 characteristics by which to validate research:

1. **Credibility** deals with the confidence that the findings of the research reflect the 'truth' of the situation under inquiry. Lincoln & Guba, (1985) state the credibility can be achieved through prolonged exposure in the field, triangulation, peer review and negative cases. Additionally, the credibility criteria can also be established through the use of member checks. This means passing the study materials and reports to the individuals who were under study, allowing them to indicate their agreement with the findings.
2. **Transferability** seeks to answer issues of generalizability that is common in quantitative studies. According to pure interpretivists, true generalizability cannot be achieved as each situation is unique. This is 'solved' by transferability by providing a detailed description of the situation under study.
3. **Dependability** attempts to deal with the issue of reliability and reproducibility. Since qualitative research settings are difficult to recreate, it falls onto the researcher to leave an audit trail of the situation, methods, and decisions made. This would allow "auditors" to assess the way in which the data has been analysed.
4. **Conformability** the auditing process carried out to establish dependability also plays a role in assessing conformability. Conformability is used to check that the results produced are not influenced by the researcher's bias to the situation. It refers to the degree to which the results can be confirmed by other individuals.

More recently, in reference to the evaluation of Grounded Theory work, (Charmaz, 2006) specifies the following evaluation criteria and questions:

1. **Credibility** Has your research achieved intimate familiarity with the setting or topic? Is there enough data to support claims? Has enough evidence been provided so readers can form independent assessments?
2. **Originality** Are your categories fresh and offer new insights? Does the research contest or extend current ideas?
3. **Resonance** Do the categories describe the completeness of the phenomenon? Does the analysis make sense to members who experience or share the circumstance?
4. **Usefulness** Does your analysis offer interpretations that can be useful to the real world? Does the research contribute to knowledge, or spark further research?

Comparing the two sets of criteria, credibility is a core criterion in assessing qualitative work. According to (Strauss & Corbin, 1998) credibility focuses on the plausibility and believability of the findings; rigor, and therefore validity and reliability is built into the research process. Hence the stress on providing detailed explanations and documentation about the analytic process taken, so other researchers may confirm and understand how new theory was developed. This thesis has provided such an audit trail as can be seen in Chapter 5, Chapter 6, and Chapter 7, thus lending to the credibility, as well as he dependability and conformability of the findings.

The quality of the research findings is further boosted by the use of triangulation (Section 4.4). Using method and data triangulation to develop the unified framework, significant overlap and relationships were uncovered between the organisation, system, and individual studies (Chapter 8). As each study draws from different data sources and perspectives, the overlaps identified validate each other's findings, thus increasing *"credibility and accountability by countering concern that a study's findings are simply an artefact of a single method"* (Patton, 2002).

It should also be noted that the individual study (Chapter 6) also made use of more traditional quantitative techniques of validation. As detailed in Section 7.4.1, a survey study was distributed, where figures for the reliability (Cronbach's Alpha) and validity (Factor loadings and Fit statistics) were produced.

9.2 Expert Evaluation

To further enhance the quality and credibility of the research findings, it would be beneficial to explore the usefulness of the framework in helping to design and implement human-centred IDMS. Ideally, this would be done through a *summative evaluation* on the effectiveness of the framework to bring about a real world change. However, this approach is unfeasible at this stage due to a lack of resources, as well as access to real world implementations that it can affect.

Therefore, this thesis has resorted to a *formative evaluation*, whereby knowledgeable experts assess the contributions and the usefulness of the findings; *"An external audit by a disinterested expert can render judgement about the quality of data collection and analysis"* (Patton, 2002). Expert reviews have been used within the HCI discipline, whereby experts assess systems to identify and highlight any shortcomings that can be improved (see for example *Usability Evaluation Methods*). The use of expert reviews fits in with the suggestions of Lincoln & Guba (1985) to use member checks to increase credibility, as well as Charmaz (2006) criterion for assessing resonance and usefulness.

A summary of the human centred framework was sent to 6 different experts, who were each asked to assess the *usefulness* and *completeness* of the findings (Anne Adams, 2001) (see Appendix VI for summaries provided to experts, and Appendix VII for the feedback received). Experts approached for review were chosen based on the criteria that they are either experienced researchers who have a well-published body of literature in the identity field (including research through the privacy or trust lenses), as well as practioners who are currently developing identity systems. It should be noted, that this pool was limited to those with whom either primary researcher is aware of. Experts were contacted via email, in which the document containing the summary of the findings and evaluation criteria were provided.

In total 4 experts were able to commit to the review, and sent in their assessment (Table 17). To ensure that experts were critical of the research, they were instructed to answer the following questions when evaluating the findings:

1. **Do the constructs asserted in the organisation sub-framework reflect real world issues that organisations deal with when implementing of an IDMS?**
2. **Can the design of an IDMS be decomposed and expressed in terms of the constructs as asserted by the system sub-framework?**
3. **Can the constructs of the system sub-framework by used to narrate the lived experience?**
4. **Do the constructs in the individual sub-framework capture individuals' concerns over, and willingness to accept a new IDMS?**
5. **Do the hypothesised relationships between the various sub-frameworks within the unified framework have merit?**
6. **Are there any other important constructs or relationships that are missing from the unified framework and its sub-frameworks?**
7. **Can the framework by used to aid system implementers to design human-centred IDMS?**
8. **Does the framework help researchers identify potential new areas of research?**
9. **Does the framework add any value to the identity field?**
10. **What improvements can be made to the framework?**

Overall experts found the framework to be useful, and that it added value to the identity field. The experts also pointed out several areas of concern/improvement; these are outlined below, and are addressed according to their themes in Section 9.3.

Table 18 Experts who reviewed the unified framework

Name	Experience	Organisation
1. Iain Henderson	Databases, Identity Management Systems	Mydex
2. Professor Andrew Adams	Social, Legal and Ethical Aspects of Computing, Computer and Network Security	Meiji University, Tokyo, Japan
3. Dr Lothar Fritsch	Information Security, Privacy enhancing technology (PET), economy of PET, IT security, electronic signatures, information hiding, mobile commerce, location-based services, design of privacy-respecting systems	Norwegian Computing Centre
4. Dr Seda Gurses	Privacy, Social Networks, Surveillance, Information Systems, Requirements Engineering	Ktholieke Universiteit Keuven

9.2.1 Expert 1 - Iain Henderson

Working with Mydex, a Community Interest Company, whose mission is to *"help individuals realise the value of their personal data… by providing individuals with Personal Data Stores and related services"*, this expert found the model to be very useful and most detailed he has seen, but has issues with some of the terminology.

9.2.1.1 Completeness

Expert 1 found no gaps with the completeness of the model, stating that *"it is the first I have seen prepared to operate at such a detailed level; most attempts bail out before the detail"*.

An issue was raised with the definitions of the system properties, where *"greater clarity could be added"* to the terms *information variability* and *intimacy* (**Concern 1A**).

9.2.1.2 Usefulness

The framework is *"a very useful one, and can be built out in many useful directions"*. However, encouraging further debate, the expert encouraged further work to bring the framework into "*operational reality*" (**Concern 1B**).

9.2.2 Expert 2 - Professor Andrew Adams

The expert agreed that the framework added much value to the identity field stating, *"the importance of the lived experience to the design of the identity systems cannot be overstated. Any work that highlights these kinds of issues well improves the field."* Suggestions were provided to further increase the completeness, and concerns were raised with respect to the utility of the framework.

9.2.2.1 Completeness

The constructs in the *system framework*, and its impacts on the *lived experience*, reflects real world issues. However, expert 2 also believed that the system framework was missing some design properties such as the *"ability of the organisation to impose the system on the target"* (**Concern 2A**).

The *individual framework* would benefit from exploring *"some finer grained"* details such as different types of *severity*; as an example expert 2 writes that the framework should consider *"the severity of a failure of the system for an individual in both, false positive and false negative terms"* (**Concern 2B**).

The constructs in the *organisation framework* also captures real concerns, but is found to be lacking of an attacker perspective;*"[The Organisation Framework] is incomplete in that it ignores any analysis of likely attackers (those seeking to suborn the system). Such attackers range from terrorists to organised criminals, to individuals seeking anonymity to elements of the organisation"* (**Concern 2C**).

The relationships present in the *unified framework* were found to have merit. Nonetheless, expert 2 feels that there are some missing dependencies, such *as "links between population comprehension and identity exposure"* (**Concern 2D**).

9.2.2.2 *Usefulness*

Overall, the *unified framework* provides a *"useful contribution"* in helping researchers identify new areas of investigation, but could be further improved by providing *"a better distinction between the framework and the application of the framework"* (**Concern 2E**).

Expert 2 also agrees that the framework presented *"a step in the right direction"* in helping implementers design human-centred IDMS.

9.2.3 Expert 3 - Dr Lothar Fritsch

The framework was found to be interesting, and inspires further research, but raised issues with the semantics of the relationships as presented in the document.

9.2.3.1 *Completeness of system framework*

"Overall, the system-based properties look usable", but properties like expert analysis are vaguely defined (**Concern 3A**). Expert 3 also suggests the exploration of the framework within large-scale distributed cloud systems that have many owners and controllers (**Concern 3B)**; correspondingly in such a scenario a new property, *"system fuzziness", was put forward* to describe the *"distributeness of the system and its owners/controllers" (Concern 3C).*

The individual framework could be improved by adding *"direct properties such as convenience, usability, and cost"* (**Concern 3D**). Expert 3 also felt that privacy and business compliance were missing from the system framework (**Concern 3E**).

Overall, the *"3 division diagram [the unified framework]"* makes sense. However, there was an issue with the semantics of the relationships, *"as they don't get defined extensively"* within the document provided to experts (**Concern 3F**).

9.2.3.2 *Usefulness*

Overall, the framework proves useful to explore new areas of research; the framework is found to accommodate for some of the experts ideas of privacy risk, and *"might be inspirational for a framework there"*.

However, the expert found it difficult to assess the usefulness of the framework in helping system designers to build human-centred IDMS. On the one hand, this is seen to stem from the experts perceived lack of proper semantics in the relationships (Section 9.2.3.1). On the other hand, the expert finds that the term *"human-centred is not obvious"*, as a proper definition had not been provided (**Concern 3G**).

Further, the expert had two suggestions that might increase usefulness. Firstly he suggests a *"technology-task-fit metric that determines how far an IDM solution is compatible with the task it should solve"* (**Concern 3H**). Secondly, *"some form of corporate risk awareness (how much do we lose on compliance breach, or upon security incidents) could be a valuable addition"* (**Concern 3I**).

9.2.4 Expert 4 - Dr Seda Gruses

An expert on privacy, social networks, surveillance, identity management systems, and the implementation of data protection principles, Seda found the framework useful for both researchers and practitioners. She was however concerned on what it means for an IDMS to be human-centred, as well as some of the generalisations that were made.

9.2.4.1 Completeness

The system framework and the design properties are *"rather interesting and helpful"*, but their definitions should be tightened, as expert 4 found them to be imprecise (**Concern 4A**). The review also expressed a desire for more articulate and clear rating mechanisms (low to high) (**Concern 4B**). A suggestion was put forward for the consideration of a new design property that captures *"the amount of control an individual has once the identity has been disclosed"*; i.e. *"capabilities similar to 'subject access rights' as defined in the data protection act"* (**Concern 4C**).

Expert 4 agrees that individual framework covers a number of very important concepts. It was put forward that work should examine *Solove's taxonomy* to capture other concerns, as well as, the consideration of Nissenbaum's concept of *contextual integrity* (**Concern 4D**). Furthermore, the expert cites the similarity of the work towards *"proportionality test of a planned technology"*, thus encouraging exploration of that field.

In the organisation framework, *authenticity* and *uniqueness* captured *"very important criteria"*. However, a flag was raised on the generalisations being made. Firstly, the expert took issue that high intimacy may not necessarily be used by organisations, as in the case where children might be protected from parents (**Concern 4E**). On the other hand, the expert found that the framework implies that uniqueness can only be provided for by biometrics, which *"is too strong of a statement"* (**Concern 4F**).

The expert also suggests exploring and including issues relating to the security of biometric; i.e. to prevent vulnerabilities in the system from being *"used to abuse the identity management system"* (**Concern 4G**).

9.2.4.2 Usefulness

The framework is indeed useful for helping researchers identify new areas of research; *"Absolutely, I really think that the work is a step forward in thinking about how to bring the lived experience of users. Future work in this direction would benefit from ways of bringing stakeholders into the evaluation of these systems, and an elaboration of the evaluation process"*.

However, expert 4 also states that she is unsure "*what to think of IDMS and human-centeredness"*, arguing that organisations implement systems for their own gain, while individuals are typically *"forced to use identity mechanisms"*. *N*evertheless, the expert still found that the framework to be useful for implementers to guide *"organisation-centric"* IDMS; *"it is an important contribution, as it puts the users of those systems as important stakeholders. I believe further work in this direction may be helpful in guiding the implementation process of 'organisation-centric' IDMS"*.

9.3 Summary of Concerns and Further Work

Overall experts agreed that the finding presented a detailed, unique, and useful approach towards developing Human Centred IDMS. However, experts also pointed out several areas in which the model can be further improved. These concerns are summarised below, along with steps to further develop them in future work.

9.3.1 Clarity of terminology

Through the evaluation, some of the experts highlighted the lack of a formal definition for the concept of a Human-Centred IDMS (concerns 3G and 4I). As of the time of writing, this shortcoming was reflected in the thesis. This has now been rectified, and a definition for a human-centred system, is provided in the initial glossary.

Experts were also concerned about the lack of clear definitions/explanations for the various constructs and relationships within the framework. This however is largely due to the space limitations in the document provided to the experts. This thesis provides richer definitions that greatly aids understanding.

Table 19 General themes from the expert reviews, and the corresponding concerns

Theme	Concerns
Clarity of terminology	Definition of "human-centred" IDMS – 3G – 4I Clarity of constructs/relationships – 1A – 3A – 3F – 4A Distinction between framework/application – 2E
Expansion of framework	New constructs/relationships – 2A (system property for impose on target) – 2B (individual perception at finer details) – 2D (relationships between other constructs) – 3C (system property for fuzziness) – 3D (individual perception of usability, cost, etc.) – 4C (system property for subject access rights) – 4D (individual perception from Solove's taxonomy) Other scenarios – 3B (cloud IDMS) – 4E (child abuse) – 4F (non-biometric IDMS)
Adding a security perspective	– 2C (attacker perspective) – 3E (organisations privacy requirements) – 4G (security of biometrics from abuse)
Operational Reality	– 1B (operational reality) – 3H (technology task fit metric) – 3I (corporate risk awareness, e.g. cost of breach)

9.3.2 Expansion of framework

Experts also encouraged further growth of the framework. For example, the experts suggested new system design properties, such as subject access rights (Concern 4C) or system fuzziness (Concern 3C). However, the analysis in this thesis was done until theoretical saturation was reached within the set of cases studied, and no new properties were being found. This is likely due to the limitation of the cases chosen for study, i.e. traditional N-IDMSs implemented by governments.

Thus while the cases reviewed here reveals core constructs which can be applied to any scenario, it is encouraged that further research should investigate other scenarios that have not been analysed, such as federated identity schemes and the system fuzziness property suggested by an expert review, or perhaps more privately owned IDMSs that would highlight the aspect of subject access rights. In exploring new designs or application areas of identity, new properties may be discovered that may help to better narrate the lived experience.

Similarly, experts also advised that more finer-grained details pertaining to individuals' perception would be beneficial (Concern 2B). Suggestions include the exploration of available taxonomies (Concern 4D), as well as the use of conventional terms such as usability, and convenience (Concern 3D). Being an exploratory study, this research steered away from traditional approaches to uncover individuals' real concerns when encountering such systems. Future work should definitely aim to integrate existing concepts, such as those proposed in this thesis that aim to explore the inclusion traditional trust constructs in determining individuals intentions to adopt IDMS (Section 6.6.1, Section **Error! Reference source not found.**)

9.3.3 Adding a security perspective

Other feedback has called for the inclusion of a security perspective (Concern 2C, 3E, and 4G). The work here has been done within the mind set of stepping away from the dominant security paradigm that has already been addressing these issues; the focus is on identity and the individual.

However, it may be useful to investigate the use of the framework, especially the system design properties, and the strategies that attackers might take to suborn the system. For example, a high number of *control points* coupled with low *subject engagement*, might indicate a greater risk from *insiders* who use the system regularly.

This avenue of research is a different line of inquiry that should be followed up in future research. Care should be taken so as to not undermine the importance of the individual, as is currently the case in the field.

9.3.4 Operational reality

Finally, Expert 1 asked if there was any strategy to bring the framework into *"operational reality"* (Concern 1B). This research presents a first phase towards a human-centred approach, seeking to describe the phenomenon of interest.

Ultimately however, it seeks to inform the design of better identity systems. This is further explored in the next Chapter. At a high level, the framework can be used to inform debates around identity systems, seeking to ensure that developers and policy makers consider all the relevant details prior to implementing an identity system; the key point is the continuous assessment of organisational requirements, its influence on system design, while ensuring that individuals concerns are addressed, as well as ensuring that the eventual lived experience does not deviate from the overall purpose of the system (Section 10.1)

At a more detailed level, the next chapter also explores the possible use of the human-centred framework within an economic context (Section 10.3). Organisations typically attempt to achieve their goals with as little money as possible; therefore, by presenting the benefits of a human-centred approach in terms of cost savings, the organisation is encouraged to implement human-centred IDMS. This thus fits in with the suggestion provided by Expert 3 to include corporate risk awareness, and how much money may be lost for breaches or non-compliance (Concern 3I).

Future work may seek to develop some kind of technology-task-fit metric as suggested by Expert 3 (Concern 3H). Some kind of weighting or scoring mechanism can help in ensuring that certain minimum thresholds of compliance, thus helping to bring human-centred systems into reality. Caution should be taken to ensure that such metrics will not take away from the lived experience; the metric should ensure that the lived experience also fits with the overall purpose.

Chapter 10: Application of Findings

Chapter 8 brought together the three different strands of research (*the system, individual, and organisation studies*) to describe a *unified framework* that provides a holistic narrative for a human-centric IDMS.

This chapter builds on the findings of this thesis by exploring its applications to influence the implementation of a human-centred IDMS. On the one hand, the *unified framework* provides designers with an implementation roadmap, ensuring a systematic evaluation system design and its implications; it ensures that the design is fit for purpose, and also includes considerations of individuals as stakeholders, while ensuring the *lived experience* does not derail from the overall purpose of the system (Section 10.1).

Alternatively, the *unified framework* can also be used to influence higher-level organisational decisions by applying the framework towards economic principles (Section 10.2). Organisations are driven by financial constraints, typically aiming to maximise return on investments, attempting to achieve their objectives while minimising costs. Faced with these constraints, it would be beneficial for IDMS designers to express human-centred solutions in economic terms, hence providing organisations with greater incentives to implement them.

10.1 Informing the IDMS Design Process

The unified model here presents a holistic narrative for the development and implementation of a human-centred IDMS. It can be used as a tool to guide designers (i.e. those who are involved with the planning and implementation of the IDMS) in developing systems that cater for the individual and the lived experience, thus maximising its impact. One possible application of the unified framework is illustrated in Figure 30 below. In this instance, the use of the framework would take place in three main phases; where organisational constructs, are analysed, then followed through to determine its impacts on initial acceptance, and finally its effects on the lived experience.

However, it should be noted that real world applications might require a rapid prototyping approach, as opposed to the waterfall model in Figure 29. In this case, the investigation continuously shifts back and forth between the various frameworks, accounting for new concerns, arguments, and possibly changing contextual factors.

Additionally, the *unified framework* can also be used to create a checklist type tool to aid in decision-making and debates. Appendix VIII provides an example of what this may look like; what is distinctive about this checklist, as opposed to strictly privacy or trust type of checklists, is the multi-disciplined approach taken, where organisations requirements quickly lead into the privacy implications of the lived experience, and onto the trust issues in citizen perception. Additionally, the checklist contains open-ended questions that emphasises the requirement of designers to fully immerse themselves in the situation, and think about the problems and implications presented by the planning and design of the system.

However, for the simplicity and to emphasise the relationships present in the unified framework, this section will explore its application in discrete steps as outlined in Figure 29.

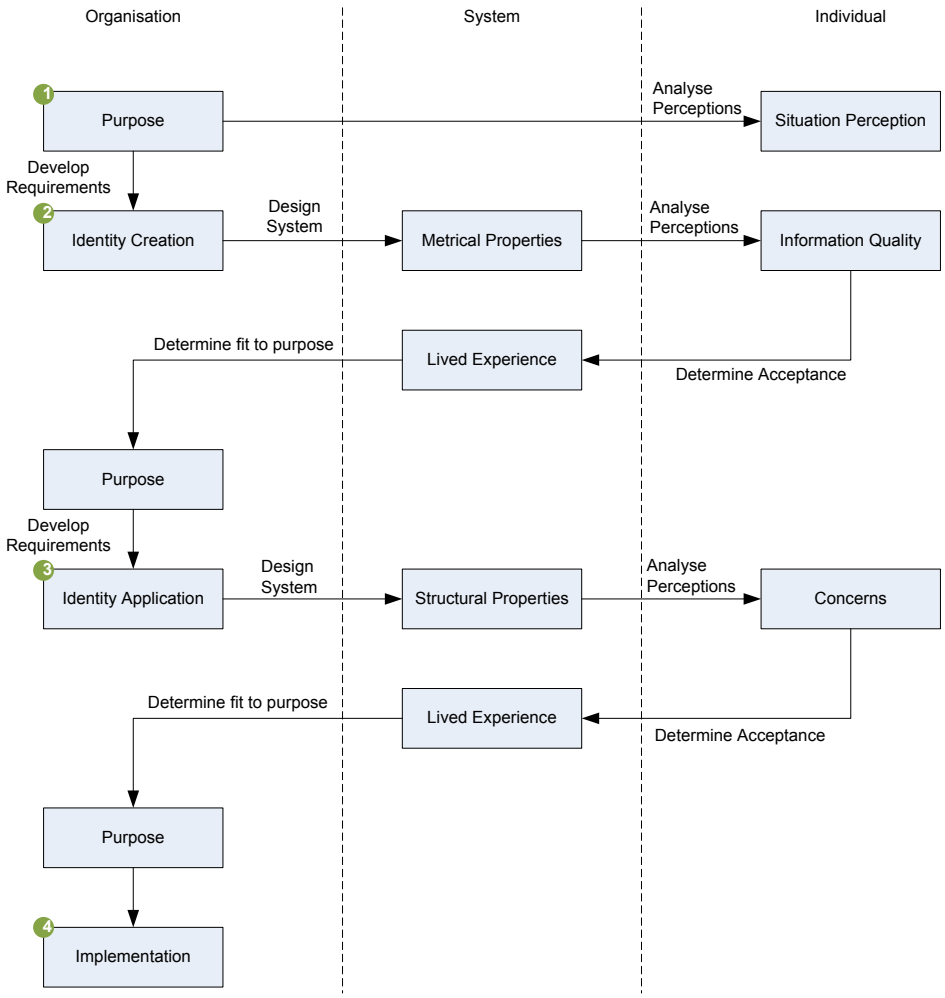


Figure 30 Application of unified framework to inform design of IDMS

The first, and most important, phase involves the setting out of the overall purpose of the IDMS, and the various tasks that it needs to support. In line with recommendations from policy experts and researchers, the initial phase requires the organisation to set out clear goals on the purpose of the system (Kent & Millett, 2002; Whitley & Hosein, 2010); the *purpose* should underwrite all decisions made about the design of the system. Once the aims and goals of the system have been specified, the organisation can then assess individual's *situation perception* on the importance of the issue being addressed; organisations want to ensure that individuals agree that the system is addressing an important issue, thus boosting the likelihood of acceptance

The next phase, involves the specification of the *authenticity* and *uniqueness* requirements. The *purpose* defined earlier, along with the *relying parties*, will here dictate the identity requirements; it will define the relevant information required to support the various relying parties in achieving their goals. This then allows system designers to determine the implications of the requirements on the *metrical properties* of the system; carefully rating each property based on the choice of personal information chosen to fulfil the *authenticity* and *uniqueness* requirements. In turn, this has implications for the individuals' *system judgement* on the usefulness of the system, acting through their perception of the overall *information quality*. System designers should attempt to identify and address any concerns raised by tracing and resolving the issue back to the system properties. Once all concerns have been addressed, designers can then focus on determining the *lived experience* as defined by the *metrical* properties; designers would carefully consider the impacts of each *metrical* property, as well as the overall combined effects. The *lived experience* defined is then compared with the originally defined *purpose* to ensure that the impacts of the system design do not go against the intentions of the system, or unintentionally create new problematic situations.

Where the second phase focused on the implications of *authenticity* and *uniqueness*, the third phase is focused on the *outcomes* of the identity usage and access. Again, informed by the purpose of the system, the implementing organisation will need to define how *relying parties* will need to access the information, in order to fulfil their goals. This in turn has implications for the *structural properties*, which can then be used to investigate individuals' *concerns* of the system, the aim being to minimise these concerns. System designers should then turn their attention to the *lived experience* as defined by the *structural properties*, building on the *metrical properties* defined in the previous stage. Again, the *lived experience* should be compared to the *purpose*, making sure that there is a proper fit, and that the IDMS will fulfil its requirements without introducing new problematic situations that can be counterproductive.

Finally, once the organisation is satisfied that individuals' would accept and use the proposed IDMS, as well as providing a *lived experience* that fits in with the overall *purpose*, the organisation can proceed to implement the system.

A point of clarification should be made regarding the investigation of the *lived experience* after its effects on initial acceptance, as presented here. Effects on *system judgement* are considered first, because it presents the first hurdle to acceptance of the system, whereas the *lived experience* can only come after acceptance. Furthermore, in comparison to assessing *system judgement*, the *lived experience* is a much more time consuming and delicate task; it may therefore be more efficient to explore acceptance, then making changes to the *metrical properties* to maximise acceptance, before attempting to define the *lived experience*. Finally, issues raised by individuals' perceptions of the system may also help to inform investigations into the *lived experience*.

10.2 Convincing Organisations - Security Economics

Apart from the application in the previous section as an analytic qualitative tool (Section 10.1), designers may also be able to apply the unified framework in a more mathematical manner through the use of Security Economic framework, which also provides the added benefit of providing organisations with financial incentives for implementing Human-Centred IDMS.

Security Economics is a growing discipline whose early work began by examining system failures within the context of perverse economic incentives; *"indeed, security mechanisms are often designed quite deliberately to shift liability, which often leads to trouble"* (R. Anderson, 2001). For example, compared to their European counterparts, US banks tend to spend less money more effectively when dealing with fraud (R. Anderson, 1993). This is largely due to different liabilities being in place, where US banks bear the responsibility to prove customers wrong when faced with fraud claims, while the burden falls on individuals within the European context; as a result US banks tend to be more diligent when implementing security systems, resulting in less occurrence of fraud.

10.2.1 Utility Theory and Transfer Functions

Later research began to apply economic theories to aid security decision-making. For example, Gordon & Loeb (2006) investigated the amount of money put into security mechanisms, and determined that the optimal upper limit of security investment would be approximately 36% of the expected loss. This branch of research brings with it *microeconomic* concepts of *trade-offs*, *cost-benefit analysis* and *utility* to aid in the decision making process. In particular, *utility theory* as described by Beautement & Pym (2010) provides an expressive framework to represent the economic consequences of security managers' preferences and decisions; Beautement & Pym (2010) provide a brief explanation of *utility* within an economic market, and the role of central banks.

> *The managers of a central bank are given, by their national governments, targets for certain key economic indicators, such as unemployment (u_t) and inflation (π_t) at time t (time can be either discrete or continuous here). Their task is to set a (e.g., monthly) sequence of controls, such as their base (interest) rates (it) so that the key indicators are sufficiently close to their targets, $\overline{u_t}$ and $\overline{\pi_t}$, respectively. Typically, using this example, the managers' policy is expressed as a utility function:*
>
> $$U_t = w_1 f_1\left(u_t - \overline{u_t}\right) + w_2 f_2\left(\pi_t - \overline{\pi_t}\right)$$
>
> *together with system equations, $u_t = s_1(i_t)$ and $\pi_t = s_2(i_t)$, expressing the dependency (among other things) of u and π on interest rates in terms of functions s1 and s2 that describe the (macro) dynamics of the economy. Two key components of this set-up are the following:*
>
> - *The weights w_1 and w_2 (typically, values between 0 and 1) that express the managers' preference between the components of the utility function—that is, which they care about more; and*
> - *The functions f_1 and f_2 that express how utility depends on deviation from target. A simple version of this set-up would take the f's to be quadratic. Quadratics conveniently express diminishing marginal returns as the indicators approach target, but make utility symmetric around target. More realistically, Linex functions usually expressed in the form $g(z) = (\exp(\alpha z) - \alpha z - 1)/\alpha^2$ are used to capture a degree of asymmetry that is parameterised by α.*

The managers' task, then, is to set a sequence of interest rates i_t such that the expected utility, $\mathrm{E}(U_t)$, remains with an acceptable range, as u_t and π_t vary, and trade-off against each other, as the sequence of rates it evolves. In general, there can of course be as many components as required in a utility function.

This function can then be applied within a security domain, where *utility* might be expressed in terms of security managers' preferences, and trade-offs between various security variables. For example, Beautement & Pym (2010) and Beresnevichiene, Pym, & Shiu (2010) express the following utility function:

1. $U_t = w_1 f_1\left(C - \overline{C}\right) + w_2 f_2\left(I - \overline{I}\right) + w_3 f_3\left(A - \overline{A}\right) + w_4 f_4\left(K - \overline{K}\right)$**; where**
    - **a.** **C** stands for confidentiality
    - **b.** **I** stands for integrity
    - **c.** **A** stands for availability
    - **d.** **K** stands for investment

Alternatively, one may also describe a *utility loss function*, which expresses the amount of loss that one would seek to minimise. In exploring the *utility* of various user password length requirements, (Arnell et al., 2011) expressed the loss in the following utility function:

2. $U_t = w_1 f_1\left(B - \overline{B}\right) + w_2 f_2\left(P - \overline{P}\right) + w_3 f_3\left(K - \overline{K}\right)$**; where**
    - **a.** **B is Breaches;** passwords become known to unauthorised individual.
    - **b.** **P is Productivity Loss;** the user's inability to access the system due to forgetting the password.
    - **c.** **K is Investment;** the provision of Help Desk Support to handle resets.

One caveat of applying the *utility function* to a security domain is the absence of *system equations* that are used to estimate the dynamics of the *key security variables* in the *utility function* (Beresnevichiene et al., 2010). Instead, security managers can create an executable system model, built around the *key security variables*, which can then be used to simulate the dynamics of the key variables; a critical component of such a model is the use of a *transfer function* that calculates the probabilities for certain outcomes (e.g. Breaches, or Productivity Losses) (Beautement & Pym, 2010).

Developing a suitable transfer function requires extensive experimental work that is beyond the scope of the work here; instead, the thesis briefly outlines the variables that could go into such a transfer function.

10.3 Economic Impacts of Human-Centred Design

In order to make a business case for supporting a *human-centred identity* solution, system designers can express the economic impacts of system design, in terms of *utility* offered by various configurations. In particular, the proposition here presents a high level overview of a set of *utility loss functions*, based on the *organisation and system framework*; the *individual framework* is not included, because it captures initial acceptance of the system, as opposed to an operational instance of an identity system.

For clarification, *utility functions* may take as many key variables as required; however, for the sake of simplicity and clarity, especially for any future attempts to model the scenario, the thesis presents small separate loss functions that captures and describes different economic aspects of human-centred IDMS.

First and foremost, the *organisation's utility loss function* presents a straightforward translation into the security economic context. Specifically, the organisations identity requirements will affect the overall occurrence of *breaches, productivity loss, and investments*, resulting in the following function:

1. **Security Utility Loss Function**

$$= w_1 f_1\left(B - \overline{B}\right) + w_2 f_2\left(P - \overline{P}\right) + w_3 f_3\left(K - \overline{K}\right)$$

   a. **Breaches (B),** is the loss incurred when individuals are wrongly given access to the system. The major variable that affects breaches is the false acceptance rate, but is also affected by population variables; therefore a transfer function to determine the probability distribution would look like:

      i. **P(B) = F(false acceptance rate, population compatibility, population size, geographic diversity, trust in authenticity)**

b. **Productivity loss (P),** which is the loss incurred when individuals are wrongly denied access to the system. The major variable that affects productivity loss is the false rejection rate. Similar to breaches, this is affected by population characteristics, as well as the trust in the authenticity of the identity. The probability distribution for occurrences of productivity loss is determined by the following transfer function:
    i. **P(P) = F(false rejection rate, population compatibility, population size, geographic diversity, trust in authenticity)**
c. **Investment (K),** which is the amount of money invested into the authenticity and uniqueness processes. Note that this may be affected by obligations on implementing various technologies, where the choice for certain technologies based on currently available systems, might reduce costs (Section *8.3.1.2*).

Moving onto the *system framework*, the economic implications of the *lived experience* must also be considered. From Chapter 5 determining the true impacts of the *lived experience* requires careful consideration of all the design properties; for simplicity this thesis reduces the outcomes of the *lived experience* to that of resistance due to a negative impact on everyday life. The system designer would therefore have to balance the trade-offs between resistance and effectiveness of the IDMS by investing in the various *design properties of the system*; this leads to a formulation of the following function:

2. **Experience Utility Loss Function**

$$= w_1 f_1\left(R - \overline{R}\right) + w_2 f_2\left(I - \overline{I}\right) + w_3 f_3\left(K - \overline{K}\right)$$

    a. **Resistance (R)** is the loss incurred due to individuals' resistance due to a negative lived experience. For example an individual might protest if the system is highly invasive (e.g. high control points and low subject engagement). R is affected by the entire set of structural and metrical properties; a transfer function to determine the probability distribution for the occurrences of resistance would be:
        i. **P(R) = F(set of all structural properties, set of all metrical properties)**

b. **Ineffectiveness (I)** is the loss incurred due to the organisation not being able to make use of the identity to fulfil its goals. For example, the organisation might not have enough access to the information in a timely manner (low control points and high subject engagement). Like R, I is affected by the entire set of structural and metrical properties; a transfer function to determine the probability distribution for the occurrences of resistance would be:
    i. **P(I) = F(set of all structural properties, set of all metrical properties)**
c. **Investment (K)** is the amount of money invested in the system design properties.

However, despite the simplification of the outcomes to two variables, the above *utility loss function* still presents a complicated model to simulate due to the large number of *structural and metrical properties* present in the *transfer functions*.

Therefore, the *utility function* can be further simplified by separating the experience of the *structural and metrical* properties into two separate *utility loss functions*. In doing so, the relationships between the two categories of properties are ignored; however, this is acceptable since the *structural properties* largely deal with the flow of information, thus primarily dealing with *resistance* due to privacy breaches; on the other hand, the *metrical properties* deal with the type of information being collected, which is largely concerned with *resistance* due to misuse/misapplication of the identity. The two separate utility functions are therefore expressed as:

3. **Structural Utility Loss Function**

$$= w_1 f_1\left(PB - \overline{PB}\right) + w_2 f_2\left(UA - \overline{UA}\right) + w_3 f_3\left(KS - \overline{KS}\right)$$

a. **Privacy Breaches (PB)** is the loss incurred due to individuals' resistance due to breaches in privacy. PB is affected by the set of structural properties; a transfer function to determine the probability distribution for the occurrences of resistance due to privacy breaches would be:
    i. **P(PB) = F(control points, subject engagement, population coverage, identity exposure)**

b. **Un-accessibility (UA)** is the loss incurred due to the organisation not being able to access the identity as it needs to. UA is affected by the set of structural properties; a transfer function to determine the probability distribution for the occurrences of un-accessibility would be:
    i. **P(UA) = F(control points, subject engagement, population coverage, identity exposure)**
c. **Investment (KS)** is the amount of money being invested into the structural design properties.

4. **Metrical Utility Loss Function**

$$= w_1 f_1\left(MA - \overline{MA}\right) + w_2 f_2\left(IE - \overline{IE}\right) + w_3 f_3\left(KM - \overline{KM}\right)$$

a. **Misapplication (MA)** is the loss incurred due to individuals stemming from the misapplications of the identity (false accusations, use of identity for other purposes, etc.). MA is affected by the metrical properties; a transfer function to determine the probability distribution for the occurrences of resistance due to privacy breaches would be:
    i. **P(MA) = F(expert involvement, population comprehension, subject coupling, information accuracy, information stability, information variability)**
b. **Ineffectiveness (IE)** is the loss incurred due to the organisation not having the information it needs to meet its objectives. IE is affected by the metrical properties; a transfer function to determine the probability distribution for the ineffectiveness of the identity information would be:
    i. **P(IE) = F(expert involvement, population comprehension, subject coupling, information accuracy, information stability, information variability)**
c. **Investment (KM)** is the amount of money being invested into the metrical design properties.

Therefore, using the *security, structural, and metrical utility loss functions*, a system designer can present a business case to cater not only for organisational requirements, but also those of the lived experience; the *utility loss functions* can be summed together to determine, and therefore minimise, the overall losses incurred. Coupled together with the individual framework to determine high initial acceptance rates, organisations can be presented with economic incentives to implement human-centred IDMS.

As a simple example to illustrate the trade off, consider an N-IDMS that aims to support the battle against crime or terrorism by requiring individuals to carry around and produce their identity document in all their daily interactions with both public and private organisations. Each use of the identity creates an audit trail that is stored on a central database, and is accessed without individuals consent.

The constant use and tracking of identity creates a system that has a *high number of control points*. Therefore, while the organisation will have access to abundant information to track and identify potential terrorists, the system design also *increases the risk of privacy breaches* occurring. The structural utility loss function will capture this increased risk of privacy breaches, expressing in terms of overall financial loss for the organisation (e.g. cost of non-compliance, court action, etc.). Therefore, the organisation can reduce these costs by *lowering the number of control points*, and thus *reducing the probability of privacy breaches* occurring.

However, this could create a situation where the organisation is unable to identify terrorists because a certain type of interaction is not recorded. The *structural utility loss* function captures this as a financial cost of not being able to identify a terrorist (e.g. tracking through other means, damage done, etc.,), due to un-accessibility of required information. Organisations thus need to balance the potential trade-offs between the costs of *privacy breaches* vs. the costs of *un-accessibility*.

It should be noted that this is not necessarily a zero sum game; reducing the probability of privacy breaches may not necessarily increase the chances of un-accessibility. The goal is to design human-centred IDMS that would be to keep potential losses to a minimum, while still ensuring that the system remains effective.

10.4 Summary and Discussion

The unified model presents a unique view into the identity process, which provides investigators with a new aid in the implementation of IDMS; the model can serve as a guide that can help to inform debate, manage perception and expectations of individuals, as well as ensuring that the overall lived experience does not derail from the overarching goal that defines the system. The application of the model, for these purposes, can be broken down into three main phases:

1. **Define Purpose.**
    i. Investigate individuals' Situation Perception based on the purpose.
2. **Based on Purpose, derive and process requirements for Identity Creation.**
    ii. Process and rate the metrical properties of the system based on the outcomes of the Identity Creation process.
    iii. Determine the effect of the metrical properties on the individuals' perception of Information Quality, and how that might affect the Judgement and Acceptance of the IDMS.
    iv. Determine the lived experience based on the metrical properties, and ensure a match to the overall purpose of the IDMS.
3. **Based on Purpose, derive and process the requirements for Identity Application.**
    v. Process and rate the structural properties of the system, based on the outcomes and requirements of the Identity Creation process.
    vi. Analyse individual concerns based on the combined structural properties, accounting for the metrical properties, and how that might affect intentions to accept the IDMS.
    vii. Determine the lived experience based on the combined structural properties, accounting for the metrical properties, ensuring a match to the overall purpose of the IDMS.

It should be noted that although the application of the model is presented here in discrete steps, the reality of the situation is likely to involve a rapid prototyping approach, where all phases may take place in tandem, quickly moving back and forth, between each framework, thus informing and encouraging debates around the IDMS.

An alternative application of the model comes from its use within a security economics context. Faced with a limited budget, organisations aim to invest their resources so as to get maximum value. Focusing on the trade-offs to the lived experience, organisations need to balance the trade-offs between the usefulness of the system for the organisations to the negative lived experience created.

By simplifying the outcomes of a negative lived experience to that of resistance/rejection, as well as isolating the effects of the *metrical and structural properties* from each other, one can generate utility loss functions that encourage organisations to explore truly human-centred approaches to IDMS. The utility functions are:

1. **Structural Utility Loss Function**

$$= w_1 f_1\left(PB - \overline{PB}\right) + w_2 f_2\left(UA - \overline{UA}\right) + w_3 f_3\left(KS - \overline{KS}\right)$$

   a. **Privacy Breaches (PB)** is the loss incurred due to individuals' resistance due to breaches in privacy.
   b. **Un-accessibility (UA)** is the loss incurred due to the organisation not being able to access the identity when and where it needs to.
   c. **Investment (KS)** is the amount of money being invested into the structural design properties.

2. **Metrical Utility Loss Function**

$$= w_1 f_1\left(MA - \overline{MA}\right) + w_2 f_2\left(IE - \overline{IE}\right) + w_3 f_3\left(KM - \overline{KM}\right)$$

   a. **Misapplication (MA)** is the loss incurred due to individuals' stemming from the misapplications of the identity.
   b. **Ineffectiveness (IE)** is the loss incurred due to the organisation not having the information it needs to meet its objectives.
   c. **Investment (KM)** is the amount of money being invested into the metrical design properties.

These can be used in conjunction with a security loss function that is created on the basis of the organisational requirements of identity, thus creating an interesting dynamic between the various functions:

3. **Security Utility Loss Function**

$$= w_1 f_1\left(B - \overline{B}\right) + w_2 f_2\left(P - \overline{P}\right) + w_3 f_3\left(K - \overline{K}\right)$$

   a. **Breaches (B)** is the loss incurred when individuals are wrongly given access to the system.
   b. **Productivity loss (P)** is the loss incurred when individuals are wrongly denied access to the system.
   c. **Investment (K)** is the amount of money invested into the authenticity and uniqueness processes.

The largest hurdle at this time is to generate the actual transfer functions for such an outcome. This is out of the scope of this thesis, but one possible way is to build a database of IDMSs, that includes a breakdown of the various system design properties as well as occurrences of events of interest (such as Privacy Breaches, Un-accessibility, Misapplications, etc.). This can then be used to generate a transfer functions that weights the system properties in relation to the events.

Thus when analysing a particular IDMS, one can take the system design rating for that particular identity system, and plug them into a Mote Carlo simulation along with the transfer function above to produce the probabilities of events occurring for that particular IDMS. These can then be feed into the utility functions to calculate the economic figures for the utility functions.

10.4.1 Future Work

The economic application of the unified model presents a key platform for further improvement and exploration. Work should attempt to focus on developing the transfer functions, so that simulations can be run; thus, a probability distribution can be developed for each trade-off, which then enables a proper quantification of the economic values.

One approach to develop the transfer functions is to explore different systems, breaking them down into the various design properties, and then determining the frequencies of privacy breaches, misapplications, ineffectiveness, and inaccessibility.

Furthermore, it may be beneficial to explore a single property as the main variable in the transfer functions, with remaining properties acting on that main variable. For example, *control points* might be taken as the central variable for the frequency of *privacy breaches*; the more an identity is accessed the more likely it is that a breach will occur. The other properties would then serve to increase or decrease the frequency of breaches as dictated by the number of *control points*; for example, low *subject engagement* would increase the number of *privacy breaches* indicated by the *control points*. Similarly, *information accuracy* might be taken as a core component for determining the *misapplications*; the other *metrical properties* would act on the base probability distribution as determined by *information accuracy*.

Chapter 11: Conclusions

Identity is a core construct that underpins all social interactions. The growth of technology-mediated communication has spurred research and development of new identity systems that attempt to leverage identity within the digital domain. However, there have been cases in which implementation of new N-IDMSs have faced resistance from individuals who are the subjects of these systems.

The review of previous research in Chapter 3 showed that researchers have been focused on the periphery constructs of usability, privacy, and trust. While these avenues of research have attempted to develop *customer/citizen centric IDMS*, these claims are largely rhetoric, viewing identity as static and utilitarian; they also fail to account for the needs of the individuals, and the overall impact of identity. The research presented in this thesis has shown that IDMS can be designed around individuals, their perceptions, and everyday lives, and that doing so is likely to lead to IDMS that are more acceptable, effective, and efficient.

By focusing on the core issue, i.e. *identity and its relationship to the individual and organisation*, this thesis has uncovered the human factors that affect the planning, implementation, and use of an IDMS. This has been developed into *human-centred IDMS framework* that provides a holistic overview around the development, perception, and impacts of an identity system.

As a first step in addressing this new focus of *human-centred* identity research, the thesis investigated the *lived experience of identity*. The results provided by this thesis uncovered several practical design aspects of IDMS that can influence individuals' lives. As well as researching long-term *lived experience*, the thesis also investigated factors determining initial acceptance or rejection of an IDMS: individuals are swayed by the perceived usefulness of an IDMS in tackling a particular problem, and their perception of the severity of that problem for society and themselves. Finally, the thesis carried out an investigation into organisational requirements of identity that affect the implementation and design of an IDMS; these concerns deal with the purpose of the identity system, which informs the authenticity and uniqueness requirements for identities enrolled within the system.

11.1 Research Question and Goals Revisited

Identity is a complex area of research that is typically tackled from the aspects of security, privacy, and trust. By bringing the focus of the research back onto identity itself, the research was guided by the following overall question:

> *What are the human factors that define or interact with identity, and how do these affect the development, implementation and use of identity management systems?*

Guided by this research question, the goals of the thesis were:

1. **Identify the relationship between the individual the IDMS.**
    a. How does the collection and use of identity affect individuals?
    b. How do individuals' perceive or choose to accept an IDMS?
2. **Identify the relationship between the organisation and the IDMS.**
    a. What are the organisational concerns around the use of an IDMS?
    b. How do organisations determine the attributes of an identity?
3. **To develop a holistic human-centred framework that describes the overall relationship between an individual, the system and the organisation.**

11.2 Overview of Studies and Results

The research was conducted in three separate studies that, taken as a whole, provide a multi-stakeholder view into the development of a *human-centred identity system*.

11.2.1 Study 1

The first study reviewed and analysed 14 different past and present N-IDMSs (Chapter 5). The results of the study are a set of system design properties that influence individuals' lived experience; i.e. the impact of the identity system on individuals' everyday lives. The design properties that emerged were distinguished into two broad categories; the *structural properties* and *metrical properties*.

The *structural properties* describe the flow of information across the entire identity eco-system, and are captured by the following properties:

1. **Control Points.** *The number of points at which an individual's identity information is accessed or used.*
2. **Subject Involvement.** *The level of participation that an individual across all the various control points.*
3. **Population Coverage.** *The percentage of the general population that is actually enrolled into the system.*
4. **Identity Exposure.** *Defines the level of control that an individual has in the presentation of his/her identity to other entities that have no right to it.*

The *metrical properties* are concerned with the type of information that is collected, stored, and used:

1. **Expert Analysis.** *The amount of manual expert involvement that is required to make an identification or authentication.*
2. **Population Comprehension.** *How well the general population understands the identification process and technologies being used.*
3. **Information Accuracy.** *The accuracy of the identity information – i.e. the reliability in producing correct matches.*
4. **Information Stability.** *The frequency with which the individual's information being collected changes over time.*
5. **Subject Coupling.** *How well the identity instantiation in the system matches the relevant partial identity in the context of use.*
6. **Information Variability.** *Refers to the possibility of the information being used for different purposes.*

11.2.2 Study 2

The second study explored individuals' initial acceptance of an IDMS (Chapter 6). Using focus groups to explore individuals' perception of identity systems, I developed a framework to predict individuals' initial trusting intention to adopt an IDMS. This framework was further refined through the use of a survey distributed to all undergraduate students in UCL; 668 responses were received and analysed using Structural Equation Modelling. The final version of the trust framework shows that individuals' acceptance of an IDMS depends on 3 main constructs, which in turn was dependent on its sub-constructs (and in one particular case one of the main constructs was influenced by the other 2 main constructs):

1. ***Situation Perception*** *describes the individual's perception of how urgently a problem needs to be addressed.*
    a. ***Severity*** *touches on the individual's perception of how serious it would be if one is affected by the problem being addressed.*
    b. ***Extent*** *captures individual's perception of how many people are affected by the problem being addressed.*
2. ***Security Concerns*** *describes the individuals' fears over the security, safety, and abuse of the identity within the IDMS.*
    a. ***Information Quality*** *which deals with individuals' perception over the accuracy and relevance of the information collected, stored, and used.*
3. ***System Judgement*** *describes the individual's perception of how useful the system will be in helping to address the problem.*
    a. ***Information Quality.***
    b. ***Situation Perception.***
    c. ***Security Concerns.***

The study also explored the effect of National Culture on individuals' perceptions. Using the cultural values as described by Hofstefe (2001) the study found that *power distance, individualism, uncertainty avoidance, and long-term orientation* influence individuals' security *concerns*. Additionally, *uncertainty avoidance* and *long-term orientation* also have a direct effect on individuals' acceptance an IDMS.

11.2.3 Study 3

Viewing identity as a strategic resource for the organisation, the third study investigated organisations' identity requirements when implementing an IDMS (Chapter 7). Using Grounded Theory analysis, the study collected and analysed data on 3 different N-IDMS implementations, each in different countries (Brunei, India, and UK). The analysis revealed that the *purpose* of the identity system drives organisations' identity requirements, informing two major activities that affect the eventual design of an IDMS:

1. ***Identity Creation*** *describes the enrolment process. This process is affected by the requirements for:*
    - ***a. Authenticity*** *determines the truthfulness of an individual's identity; i.e. the choice of biographical information which is affected by:*
        - ***i. Universality*** *is the percentage of the target population that already possesses accepted forms of identity documents.*
        - ***ii. Intimacy*** *captures the percentage of the population that is already known to the organisation, and can thus vouch for the individual.*
    - ***b. Uniqueness*** *ensures that an individual does not enrol within a system more than once. Typically done using biometrics, which is mediated by:*
        - ***i. Obligations****. Requirements that an organisation has to consider (international obligations, current practices).*
        - ***ii. Performance****. Accuracy of the biometric in producing matches (accuracy, human readability).*
        - ***iii. Population****. The factors that affect performance of the biometric (size, compatibility, geographic diversity).*

2. ***Identity use*** *is concerned with the process of establishing the mechanism that enables relying parties to access and use identities in the system.*

    a. ***Purpose****. Describes the problem that the IDMS is meant to support.*

    b. ***Relying Parties. T****he various users that need access to the identity to complete a task (organisations, individual).*

    c. ***Objectives****. Relying parties' intention and requirements to use the identity (enablement, proof).*

    d. ***Conditions.*** *The situational factors under which the relying parties operate (risk level, timeliness).*

    e. ***Accessibility.*** *The manner in which the organisation will access the identity (information set, locality, direction)*

Table 20 Summary of studies, approaches, and results in this thesis

	Study 1	Study 2	Study 3
Chapter	5	6	7
Focus	System	Individual	Organisation
Research Goal	1a	1b	2a, 2b
Methods	Historiography Thematic Analysis	Focus Groups Grounded theory Factor Analysis Structural Equation Modelling	Documents and Interviews Grounded theory
Determinant	Lived Experience	Initial Acceptance	System Design
Results/Variables	Structural Properties ▪ Control Points ▪ Subject Engagement ▪ Population Coverage ▪ Identity Exposure Metrical Properties ▪ Expert analysis ▪ Population Comprehension ▪ Subject Coupling ▪ Information Accuracy ▪ Information Stability ▪ Information Variability	Acceptance ▪ Situation Perception ▪ Concerns ▪ System Judgement ▪ *Uncertainty Avoidance (culture)* ▪ *Long-Term Orientation (culture)* Situation Perception ▪ Severity ▪ Extent Concerns ▪ Information Quality ▪ *Power Distance (culture)* ▪ *Individualism (culture)* ▪ *Uncertainty Avoidance (culture)* ▪ *Long-Term Orientation (culture)* System Judgement ▪ Information Quality ▪ Situation Perception ▪ Concerns	Authenticity - determines biographical information ▪ Intimacy / Universality Uniqueness - determines biometric information ▪ Obligations (International, Current Practices) ▪ Performance (Accuracy, Readability) ○ Population (Size, Compatibility, Geographic Diversity) Purpose - determines identity access policies ▪ Relying Parties ▪ Objective ▪ Conditions ▪ Accessibility

11.3 Contributions for Researchers: From User-centric to Human-Centric Identity

This research has produced new substantive knowledge on identity. It presents a point of departure from the traditional approaches that focus on usability of IDMS, and encourages researches to examine the relationship between individuals and the identity system. Traditional 'user-centric' perspectives of identity reduce the individual to a functional component within the organisations' overall 'work system'; what matters is the system-individual 'fit' to achieve *desired performance* (Taylor & Coutaz, 1994; Whitefield, Wilson, & Dowell, 1991). Research thus ignores the effect that identity systems have on individuals, which means issues such as users' mental and physical workload and sensitivity.

While IDMS should be usable, it is an insufficient perspective to capture the impact of identity on individuals. Researchers are encouraged to take a broader view of the problem, and investigate individuals' overall experience, not just functional points of interaction. As opposed to user-centric approaches that focus on ease-of-use, identity research needs to take a human-centred approach that designs for individuals' concerns, as well as the implications of the system on their everyday lives. The implications of this approach for researchers are outlined below:

11.3.1 Privacy – from confidentiality to the lived experience

As IDMS by their nature deal with personal information, the privacy literature has been dominated by issues of informational privacy, and hence concentrates on solutions of confidentiality to ensure privacy. However, current research knows little about how identity can affect individuals in the first place. What good are the privacy protections if one does not understand the effects of identity? Some researchers have mirrored these concerns stating that "*identity related issues cannot be dealt with from a privacy-perspective*" (Gutwirth, 2009), or that we "*need to move beyond discussions about privacy, and move into a full fledge discussion of identity*" (Lusili, Maghiros, & Bacigalupo, 2009).

In exploring the *lived experience* of identity, this thesis opens up a whole new perspective. Moving pass the issues of privacy and confidentiality, the focus is on the impact of identity use on individuals' everyday lives, and thus its effect on individuals' behaviour and freedoms. The *structural* and *metrical properties*, when taken together, help us to describe the effect on the lived experience.

In the Poor Law system (Section 2.2.1.2 and Section 5.2.1.1), the government attempted to control the issue of false begging by requiring individuals to register with the government. Upon registration, beggars would be presented with an identification badge that they were required to wear on the sleeves at all times, signalling to others that they had a right to beg. However, the system backfired; true beggars chose not register, and instead lived a life of crime. This was because the system design was highly targeted in nature (*low population coverage)*, required individuals to wear the badges at all times (*high number of Control Points* and *high Subject Engagement*), which meant that the identity was broadcast for everyone to see (*high Identity Exposure*). Thus this combination of system properties led to the system creating feelings of shame for individuals', and hence their reluctance to use it.

As another example, the assumed infallibility of fingerprint identification, for criminal identification, brings with it dangers of false convictions (Cole 2001). Fingerprints pulled from crime scenes are typically of low quality (*low Information Accuracy*), and requires experts to make decisions on fingerprint matches (*high Expert Analysis*). In addition, the general population does not understand how this process works (*low Population Comprehension*), relying on expert's analysis, while also typically equating a fingerprint match as proof of guilt (*low Subject Coupling*). This leads to a situation where individuals are wrongly accused or convicted because of incorrect subjective judgements of experts, based on inaccurate information that individuals do not understand. This effectively removes an individual's ability to resist such accusations; even with safeguards the McKie case (Section 2.2.4.3 and Section 5.2.3.2.2) shows how easy it is to subvert the system, when experts make a false positive identification of an individual to a crime scene fingerprint sample.

Therefore, researchers need to look beyond the traditional *informational privacy* dimension. We need to examine how identity and the design of an IDMS truly affect individuals' lives. Privacy is important, but is too narrow a concept to address these questions. Research needs to look at the lived experience of identity, how the concept further, and how it can integrate this into current literature and privacy models.

11.3.2 Trust – From beliefs to risk perceptions

With the exception of (Li, 2004), there has been no in-depth investigation on the individuals' trusting intentions towards IDMS. However, as with most other trust research in computer science, the emphasis of previous research has been on the exploration of trust through individuals' general attitudes and beliefs. The root of all these trust research is largely based on Fishbein & Ajzen's (1975) *Theory of Reasoned Action (TRA)* that individuals' intention to trust is built on:

1. **Attitude.** A person's favourable or *"unfavourableness towards an action" (Fishbein & Ajzen, 1975).*
2. **Subjective norm.** An individual's preconceptions on whether the people closest to him/her think that the action should be carried out.

However, attitude and subjective norms do not provide any information on how the specific design details of an identity system influences individuals' perceptions, and thus their trusting intentions; i.e. the TRA constructs are focused on individuals' general feelings, and not their assessments of the identity system.

This is where the research here differs from the traditional approach, focusing on how the individuals perceive and judge the details of an identity system. Specifically, the research has revealed that individuals' intention to trust an identity system is based on *situation perception, system judgement,* and *security concerns*. Situation Perception captures individuals' assessment on the importance of addressing the problem situation that the IDMS is targeted at. The more *severe* the problem is perceived to be, and the greater the *extent* of the population perceived to be affected by it, the greater the *situation perception* and thus the greater the willingness to accept the system.

Meanwhile *concerns* have a negative influence on trusting intentions. The more individuals believe that their identity information is vulnerable to *unauthorised access* (by hackers or *insiders)*, or fearing *future unpredictability* in how the organisation might use their information (e.g. function creep); the less likely individuals are willing to trust and adopt an IDMS. Furthermore, *concerns* are also affected by the *information quality*, which deals with individuals overall perception of the accuracy and relevance of the information collected and stored in the system. As the perception of *information quality* decreases, individuals' *concerns* increases, thus reducing their *trusting intentions*.

Finally, *system judgement* deals with individuals' perception on the usefulness of the system in tackling the situation. A positive judgement of the system implies that individuals' perceive the system to be a useful tool in addressing the problem, and thus increases individuals willingness to trust the system. *System judgement* is positively influenced by *situation perception*, and negatively affected by *concerns*, and *information quality*.

When compared to traditional trust concepts such as *attitudes*, the findings of this research provide more relevant feedback on the relationship between the system design and individuals' trusting intentions. For example, organisations can focus on building individuals' trust by addressing individuals' concerns, or ensuring that the quality of the identity being collected and stored meets individuals' expectations. Traditional approaches are disconnected from the system itself, and as such, provide limited avenues to design trust-worthy systems. In order to create more trustworthy IDMS, research needs to identify which parts of the system affect the individuals' risk perceptions, and thus intentions to trust/adopt and IDMS. Researchers should therefore, seek to explore how the system design contributes to individuals' *perceived risk*, and thus intentions to adopt an IDMS.

11.4 Contributions for Practitioners: Designing Fit-for-purpose IDMS

The findings of this thesis also have practical contributions that can assist organisations in building more effective human-centred IDMSs. Key to these contributions is the importance in acknowledging that the implementation of successful IDMSs depends on the organisation defining a clear *purpose* for the system.

Purpose drives everything; as illustrated in the organisation framework, *purpose* dictates the organisation's identity information requirements (*authenticity* and *uniqueness*), as well as the way in which *relying parties* will access the identity. Failure to consider the purpose of the system will lead to ineffective implementations that either does not meet the requirements needed to achieve the desired objectives, or conversely would result in systems that include unnecessary functionality or technology.

11.4.1 Designing for individuals

As with the contributions for researchers, organisations are encouraged to include individuals in the process of designing the IDMS. Organisations should not only look at their own identity requirements, but take a more holistic view of IDMS. It must be recognised that organisations' requirements determine the system design, which in turn determines individuals' positive or negative *perception* of the system, as well as the eventual *lived experience* created.

To encourage adoption, organisations must create trustworthy IDMSs that address concerns of the population. Low trust and acceptance would result in more expenses to convince/enforce individuals to use the system, and failing that, organisations may be forced to abandon the system altogether.

Similarly, the design of the system will influence individuals' *lived experience* over time. IDMS designers are encouraged to map out and determine the impacts that the system has on the individuals' everyday lives during the design phase. It must be ensured that the *lived experience* created matches with the objectives of the organisations, and does not derail from the overall *purpose* of the IDMS.

11.4.2 Identity Creation: Verification of Authenticity and Uniqueness

In the literature, enrolment of individuals into the system is a key phase in the implementation and use of an IDMS. As part of this process, the literature typically describes a verification process carried out by the organisation to ensure that the individual is who he claims to be.

The results of this research have uncovered much more detail on the identity verification process, outlining the factors that influence organisations' choice and source of information from the individual. Specifically, the framework breaks down the traditional identity verification process into *authenticity* and *uniqueness that* helps organisations better plan the identity creation process, and thus the overall information collected and stored.

Authenticity is described as the truthfulness of an identity created within the IDMS. The *authenticity* of an individual's identity is ensured by confirming the truthfulness of his/her biographical information (e.g. name, age, address) against various different sources. The collection of biographical information can be achieved through a *document-based* or *introducer-based* approach. The *document-based* approach requires a high level of *universality*, which refers to the percentage of the targeted population who are in possession of widely accepted forms of identity documents. Thus, the greater the universality, the greater the number of people who have documents that prove their identity (e.g. passport, driving license), and thus the more confident the organization can be in relying on documentation for proving authenticity of identity.

On the other hand, low *universality* implies that an organisation cannot rely on documentation for authenticity. In such cases, the organization can turn towards an *introducer-based* approach, provided that there is a high level of *intimacy* with the target population; *intimacy* captures how much of the targeted population is already known to the implementing organisation, and thus enrolled individuals can vouch for the other individuals' identity. A high level of *intimacy* means that the organisation already possess a large set of trusted identities, and thus can opt for a transitive trust scheme, whereby a known registered individual can vouch for an unknown individual enrolling into the system (e.g. parents vouching for children).

Other than *authenticity*, organisations also need to ensure *uniqueness* of identities so that an individual cannot enrol more than once. This is usually done through the collection of biometrics, the choice of which is mediated by an organisation's obligations (international standards and current practices).Thus, for example, an IDMS designed to support individual identification during travel, would need to implement the internationally agreed biometric standard, thus ensuring interoperability across all countries.

Further the organisation must also consider the *performance* of the biometric in producing correct matches *(accuracy,* and *human readability*). For example, a system designed to support national security functions require a high level of *accuracy* ensuring that there are few false positives. The *performance* measures should also take into account the effect of the real world *population* (*size, compatibility, geographic diversity*). For example, if the targeted population largely consist of individuals that do a lot of manual labour, then there is low *compatibility* with fingerprint biometrics (since manual work wears down the fingerprints).

Therefore, when designing the enrolment process, organisations are encouraged to look beyond the simple act of identity verification, and go deeper to explore their *authenticity* and *uniqueness* requirements, as well as the factors that influence the suitability of the biographical and biometric information that should be collected, processed, and stored during enrolment.

11.4.3 Engaging Relying Parties

The framework also highlights the importance of the continuous engagement with all the relevant Relying Parties, to ensure that the right infrastructure and access protocols are built into the IDMS, thus increasing the uptake and use of the system. In the Indian N-IDMS case study (Section 7.2.3), the government sought close collaboration with several Relying Parties, to the extent that new services such as mobile banking have been planned. Contrast that to the Bruneian case study, where the lack of interaction with third parties has meant that the multi-purpose function of the N-IDMS has not been realised. Thus failure to identify and engage with relying parties will lead to IDMSs that are not widely adopted for use by third parties, and are likely to be ineffective

As detailed in the organisation framework, designing around Relying Parties also helps organisations to develop better access policies to suit Relying Parties needs. For instance, parties that operate in high risk *conditions,* with the *objective* of disabling individuals from performing actions, would require a high degree of *accessibility* to system and the identity information on it. An anti-terror unit would need to remotely access individuals' entire history of transactions; this would imply the need of a centralised database, as well as a networked infrastructure to the system. On the other hand, Relying Parties that work in low risk *conditions*, and whose *objective* is to enable individuals to carry out a simple action, may only need a comparatively low level of *access* to the system. For example, picking up a parcel at a post office would not need to access identity remotely, and thus place no such requirements on the design of the system.

Thus identity access policies, as well as overall IDMS design, are influenced by *relying parties* and their need to access identity in pursuit of their respective objectives. Establishing a relationship with these *relying parties* enables the organisation to better understand their requirements, working conditions, and concerns; these can then be designed into the system, thus ensuring maximum take up of the IDMS. Therefore, to ensure the successful implementation of an IDMS, organisations are encouraged engage with relying parties, and to design identity systems to fill all their requirements. Failure to do so would lead to implementation that are not widely adopted by third parties, and will thus likely be ineffective.

11.5 Discussion and Critical Review

While the thesis has produced new and unique insights based on empirical data, there are certain areas in which the research here is limited, and can act as platforms for further improvement. These are:

1. **The exploratory and descriptive nature of the research**
2. **The breadth and complexity of research and findings**
3. **The limitation of the research to N-IDMS**
4. **The subjectivity required to apply parts of the framework**

The findings of the research here were produced through a highly descriptive and narrative process. It could be argued that the results are too dependent on qualitative data, and not sufficiently validated. However, to develop a rich picture of the identity, exploration of qualitative material is more suitable than testing of predefined hypothesis using quantitative methods. Furthermore, grounded theory (the main method of investigation used) presents a scientific and structured approach to the collection and analysis of qualitative data, leading to a framework that can be subjected to empirical testing. It should also be noted that, despite being conducted in an exploratory manner, the individual study findings were supported and refined using statistical methods (Section 6.4.1); this was the case, because the individual study naturally lent itself to the exploration of acceptance and perceptions through the use of surveys. The research has taken other explicit steps to ensure validity. This includes the use of data and method triangulation to show that results from the different studies and perspectives are compatible, thus lending the findings validity (Section 4.4 and Section 8.2). Finally, a formative evaluation of the unified framework was also conducted through the use of Expert Analysis (all of which were required to be critical of the usefulness and completeness of the unified framework), which overall finding it to be a useful contribution to the field (Section 9.2).

The breadth and complexity of the framework produced may also serve as a point of concern. However, identity itself is a complex multidisciplinary and multi-stakeholder field. As such, any attempt to truly capture the scene in its fullest will undoubtedly be complex; in capturing this complexity, the relationships captured between the various perspectives, helps to develop a more complete understanding of the field. This also explains the breadth of the research undertaken. Taking a new approach towards identity, it was necessary for the research to cast a wide net instead of pre-emptively deciding to focus on a specific area of study. How do we know what to study, if we don't know what is involved? Thus the research here acts as an initial foundation for the pursuit of other research into genuinely human-centred IDMS.

The research presented here is largely focused on identity within the context of N-IDMS implemented by government agencies, which may imply a narrow scope of possible application. However, the findings from the *lived experience* of identity were successfully applied within non-governmental contexts (Section 5.3.1); providing a narrative that explains the reactions and outcomes within a social networking and personalised advertising context, thus illustrating the generalizability of the *lived experience* framework to non N-IDMS scenarios. When examining the *individual acceptance* framework, the constructs appear to be general enough to be extended beyond the N-IDMS context. However, the *organisational requirement* framework may present some incompatibilities; specifically, the use of biometrics in all three cases under analysis, and its inclusion in the framework may restrict its applicability to other contexts. Not all organisations might require, or have the resources to implement such a high level of assurance for *uniqueness*; it is also probable that some organisations may take the proof of *authenticity* as a sign of *uniqueness*. In these cases, the factors that determine *uniqueness* are not relevant. However, the constructs that govern the overall *biographical information and identity access policies* are still pertinent in all contexts, and may be applied.

Finally, a weakness that is specifically borne out of the *lived experience* framework is the subjectivity required to fully utilise the framework and its properties. What is a *high level of subject engagement*? What is a *low number of control points*? While there is an element of rating taking place, one would not be able to simply assign weights of importance to each property; there is a degree of interpretation required, and different individuals might perceive things differently, which can lead to a source of inconsistent results. Furthermore, this may be affected by the *contextual integrity* (Nissenbaum, 2004) where what is considered high or low is affected by the norms of the environment into which the system is implemented.

Further still, interpreting the effects of each property may require careful consideration, as the effects and relationships of one property to another may slightly differ according to the contexts. A 'high' or 'low' of rating for each property does not automatically indicate a good or bad outcome. However, while the level of subjectivity required may be perceived as a stumbling block, it should be seen as a strength; proper application the framework requires that the designer immerse him/herself in the situation that the system will be used; proper assessment of the various properties requires thought and reflection, analysing the system from the point of view of individuals and society that are affected by it. This is a breakaway from the administrative-centric perspectives, which removes a system implementer from the context. The system properties serve to re-embed the design process into the reality of the situation in which the IDMS is implemented.

11.6 Future Work

While this thesis presents a unique approach to human-centred identity, there is more research needed. The system framework would benefit from the exploration of new design properties that could further help to develop the *lived experience*. Furthermore, it would be beneficial if a complete mapping of between the design properties and various outcomes were to be developed; such a mapping would make the application of the framework much more effective and useable (Section 5.4.1).

The individual framework would benefit from a further expansion of the quantitative survey study. The survey conducted in this study was exploratory, seeking to improve the first proposed individual framework, and a validation study is needed. Similarly the effects of culture on the lived experience would benefit from a larger quantitative based exploration, as opposed its qualitative applications in this thesis. Future work may attempt to incorporate the findings into traditional trust models, thus further improving the explanatory power of the individual framework (Section 6.6.1).

The organisation framework would benefit from an investigation of other cases that differ from the biometric based N-IDMS analysed here. Thus, future work could look towards investigating non-biometric systems, and its impacts on organisational *uniqueness* requirements (Section 7.5.1).

Meanwhile, the unified framework would benefit from the exploration of new relationships between the different perspectives. Work could also be done to investigate the fine grained details of known relationships (Section 8.5.1).

Other work could further expand the applicability of the unified framework through the development of the economic utility functions, and the probability distributions that feed into the transfer functions (Section 10.4.1). Alternatively, the development of some kind of computing design tool, based on the unified framework, could be developed to help ease the application of the research into real world scenarios.

However, above all it would be highly beneficial to take this research beyond just exploration. Future work should attempt to apply these findings to influence the implementation of new IDMS. Using methods such as Action Research, the framework can be further developed, ensuring its on-going relevance to the real world, while producing real change through the development of effective human-centred IDMS.

New research should also be open to other perspectives. For example, one of the suggestions that came out of the expert evaluation calls for the inclusion of attackers in the framework. The inclusion of this perspective in the framework can help to identify weak points in the system, and how that is affected by the organisation's identity requirements, as well as the design of the IDMS.

Ultimately, there needs to be a realisation that identity is a fundamental right to all individuals; every social interaction is defined by who we are. As such IDMS should be explored, researched, and built around this realisation. In so doing, the focus of investigations and discussions should fall upon identity as the central theme, and not just as a periphery to other concepts such as trust or privacy. This thesis presents an effort to move identity discussions towards this viewpoint. Failure to do so will result in highly utilitarian systems that do not respect individuals, constantly invade privacy, and may fundamentally disempower individuals from living freely.

Appendix I: References

Abramson, R., Rahman, S., & Buckley, P. (2005). Tricks and traps in structural equation modelling: A GEM Australia example using AMOS Graphics. *ABBSA Conference* (pp. 558–599). Retrieved from http://www.swin.edu.au/hed/test/gem/reports/Abramson_SEM_paper.pdf

Adams, A, & Sasse, M. (2001). *Privacy in multimedia communications : Protecting users*. Retrieved from http://citeseer.ist.psu.edu/adams01privacy.html

Adams, Anne. (2001). *Users perception of privacy in multimedia communication*. University College London.

Adams, Anne, Lunt, P., & Cairns, P. (2008). A qualitative approach to HCI research. In P. Cairns & A. L. Cox (Eds.), *Research methods for human-computer interaction*. Cambridge, UK: Cambridge University Press.

Agar, J. (2001). Modern horrors: British identity and identity cards. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey 08540: Princeton University Press.

Agar, J. (2005). *Identity cards in Britain: past experience and policy implications*. *Identity cards in Britain: past experience and policy implications, by Jon Agar*. Retrieved from http://www.historyandpolicy.org/papers/policy-paper-33.html

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl (Ed.), *Action control, from cognition to behavior*. Berlin: Springer-Verlag.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Al-Raisi, A. N., & Al-Khouri, A. M. (2008). Iris recognition and the challenge of homeland and border control security in UAE. *Telematics and Informatics*, *25*(2), 117–132. doi:10.1016/j.tele.2006.06.005

Anderson, B. (1991). *Imagined communities : reflections on the origin and spread of nationalism*. London; New York: Verso.

Anderson, Brown, I., Clayton, R., Dowty, T., Korff, D., & Munro, E. (2006). *Childrens databases – safety and privacy*. Retrieved from http://eprints.ucl.ac.uk/3878/

Anderson, & Dourish, P. (2005). Situated Privaces: Do you know where you mother [trucker] is? Las Vegas, Nevada.

Anderson, R. (1993). Why cryptosystems fail. *1st ACM conference on Computer and communications security - CCS '93* (pp. 215–227). New York, USA: ACM Press. doi:10.1145/168588.168615

Anderson, R. (2001). Why information security is hard - an economic perspective. *Seventeenth Annual Computer Security Applications Conference*, 358–365. doi:10.1109/ACSAC.2001.991552

Arnell, S., Beautement, A., Inglesant, P., Monahan, B., Pym, D., & Sasse, A. (2011). *Systematic decision making in security management: modelling password usage and support* (pp. 1–31). Retrieved from http://www.hpl.hp.com/techreports/2011/HPL-2011-36.html

Arora, S. (2008). National e-ID card schemes: a european overview. *Information Security Technical Report*, *13*(2), 46–53. doi:10.1016/j.istr.2008.08.002

Ashbourn, J. (2000). *Biometrics : advanced identity verification; the complete guide*. London; New York: Springer.

Ashbourn, J. (2004). *Practical biometrics: from aspiration to implementation*. London, England: Springer.

BBC. (1999). Robbery conviction overturned. *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/uk/258367.stm

BBC. (2000a, January). Transcript: finger of suspicion. *BBC Frontline Scotland*. Retrieved from http://news.bbc.co.uk/1/hi/scotland/605129.stm

BBC. (2000b, June). Greek protest over ID cards. *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/world/europe/791084.stm

BBC. (2002). Japan launches ID scheme. *BBC News*. London, England. Retrieved from http://news.bbc.co.uk/1/hi/world/asia-pacific/2173003.stm

BBC. (2003, December 31). Brazil to fingerprint US citizens. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/americas/3358627.stm

BBC. (2006, May 12). Kin search "could trap criminals." *BBC News*.

BBC. (2007, October). Transcript: give us your DNA. *BBC Panorama*. Retrieved from http://news.bbc.co.uk/1/hi/programmes/panorama/7040162.stm

BBC. (2008a, March). Rethink on identity cards plans. *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/7280495.stm

BBC. (2008b, August 5). McCann DNA evidence "exaggerated." *BBC News*.

BBC. (2008c, December). DNA database "breach of rights." *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/7764069.stm

BBC. (2009, July 17). Facebook "breaches Canadian law." *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/world/americas/8155367.stm

BBC. (2010a). Identity cards scheme will be axed "within 100 days." *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/8707355.stm

BBC. (2010b). World of Warcraft maker to end anonymous forum logins. *BBC News*. Retrieved from http://www.bbc.co.uk/news/10543100

BBC. (2011a, February 11). DNA profiles to be deleted from police database. *BBC News*. Retrieved from http://www.bbc.co.uk/news/uk-12433116

BBC. (2011b, February 16). Manchester Airport facial recognition gates suspended. *BBC News*. Manchester. Retrieved from http://www.bbc.co.uk/news/uk-england-manchester-12482156

Backhouse, J., & Halperin, R. (2007). *A survey on EU citizens Trust in ID systems and authorities* (pp. 1–31). Retrieved from http://www.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf

Bannur, J. (2010). *Proof of concept learnings*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189

Banse, P. (2008). E-Personalausweis soll Pseudonym-Funktion erhalten. *Heise Online*. Retrieved from http://www.heise.de/newsticker/meldung/E-Personalausweis-soll-Pseudonym-Funktion-erhalten-179956.html

Bauer, M., Meints, M., & Hansen, M. (2005). *Structured overview on prototypes and concepts of Identity Management Systems*. Retrieved from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf

Bauer, T., & Zimmermann, K. (1997). Integrating the East: the labour market effects of immigration. In S. W. Black (Ed.), *Europe's Economy Looks East: Implications for Germany and the European Union* (p. 381). Cambridge University Press.

Beaumont, C. (2010). Facebook admits “inadvertent” privacy breach. *The Telegraph*. London, England. Retrieved from http://www.telegraph.co.uk/technology/facebook/8070513/Facebook-admits-inadvertent-privacy-breach.html

Beautement, A., & Pym, D. (2010). Structured systems economics for security management. *Ninth Workshop on the Economics of Information Security* (pp. 1–20). Harvard University. doi:10.1.1.165.4280

Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, *17*(2), 165–176. doi:10.1016/j.jsis.2007.12.002

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, *20*(5), 313–324. Retrieved from http://www.informaworld.com/10.1080/01972240490507956

Bellotti, V., & Sellen, A. (1993). Design for Privacy in Ubiquitous Computing Environments. *Third European Conference on Computer Supported Cooperative Work* (p. 7792). Kluwer. Retrieved from citeseer.ist.psu.edu/bellotti93design.html

Bender, J. (2008). The German eID-Card. *Second ENISA workshop on next generation Electronic Identity*. Federal Office for Information Security. Retrieved from http://www.eema.org/index.cfm?fuseaction=events.content&cmid=368

Bennetto, J. (2000, June 26). Police refuse to take DNA tests for database. *The Independent*.

Beresnevichiene, Y., Pym, D., & Shiu, S. (2010). Decision support for systems security investment. *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*, 118–125. doi:10.1109/NOMSW.2010.5486590

Berg, B. L. (2001). *Qualitative research methods for the social sciences*. Boston: Allyn and Bacon.

Bhattacharya, S. (2004, April). Killer convicted thanks to relatives DNA. *New Scientist*. New Scientist. Retrieved from http://www.newscientist.com/article/dn4908

Bieber, F. R. (2004). Science and technology of forensic dna profiling. In D. Lazer (Ed.), *DNA and the criminal justice system : the technology of justice*. Cambridge, Mass.: MIT Press.

Biometric Technology Today. (2007, January). UKs Project IRIS comes under fire. *Biometric Technology Today*, *15*(1), 1. doi:10.1016/S0969-4765(07)70021-8

Birch, D. G. W. (2009). Victorian values: Politicians and the public incorrectly see security and privacy as opposites. *Information Security Technical Report*, *14*(3), 143–145. doi:10.1016/j.istr.2009.10.006

Blunkett, D. (2003). *Identity Cards: the next steps*. London, England. Retrieved from http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/978.htm?advanced=&searchoperator=&searchmodifier=&verb=&search_date_from=&search_date_to=&stage=&search_event_subject=&search_category=&search_query=&search_scope=&search_group=&varChunk=

Braithwaite, J. (1989). *Crime: Shame and reintegration*. Cambridge University Press.

Brubaker, R., & Cooper, F. (2000). Beyond Identity. *Theory and Society*, *29*(1), 1–47. Retrieved from http://www.jstor.org/stable/3108478

Brudirect. (2002). Sultanates Smart Cards to get smarter. *Brudirect*. Retrieved December 20, 2010, from http://www.brudirect.com/DailyInfo/News/Archive/June02/230602/nite06.htm

Brunei Immigration & National Registration Department. (2005). About BruNIR. Retrieved from http://www.immigration.gov.bn/official/about bruinr.html

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook 6*, 206–249. Retrieved from http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6T7T-445G671-5&_user=125795&_coverDate=12/31/2001&_rdoc=1&_fmt=high&_orig=search&_origin=search&_sort=d&_docanchor=&view=c&_searchStrId=1645241831&_rerunOrigin=google&_acct=C000010182&_version=1&_urlVersion=0&_userid=125795&md5=be04000a7e31bb5609ab70a226903684&searchtype=a#bbib16

Burkert, H. (1997). Privacy-enhancing technologies: typology, critique, vision. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: the new landscape*. Massachusetts: MIT Press. Retrieved from http://cognet.mit.edu/library/books/mitpress/0262511010/cache/chpt4.pdf

Burnham, A. (2006, February). Cost of Identity Fraud to the United Kingdom economy. London, England: Home Office. Retrieved from http://www.callcredit.co.uk/download/cost-of-identity-fraud-to-the-United-Kingdom-economy.pdf

Camenisch, J., Shelat, A., Sommer, D., Fischer-Hübner, S., Hansen, M., Krasemann, H., Lacoste, G., et al. (2005). Privacy and identity management for everyone. *The 2005 workshop on Digital identity management* (pp. 20–27). Fairfax, USA: ACM. doi:10.1145/1102486.1102491

Cameron, K. (2005). The laws of Identity. Microsoft Corporation. Retrieved from http://www.identityblog.com/?page_id=354

Camp, L. J. (2004a). Digital identity. *Technology and Society Magazine, IEEE*, *23*(3), 34–41. doi:10.1109/MTAS.2004.1337889

Camp, L. J. (2004b). Identity in digital government. *papers.ssrn.com*. Cambridge, Massechutes: Harvard University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=615187

Campbell, A. (2011). *The Fingerprint Inquiry Report*. Edingburh, Scotland.

Caplan, J., & Torpey, J. (2001). *Documenting individual identity*. Princeton University Press.

Carroll, J. M. (2000). *Making use scenario-based design of human-computer interactions*. Cambridge, Massechutes: MIT Press.

Carroll, W. C. (1996). *Fat king, lean beggar : representations of poverty in the age of Shakespeare*. Ithaca: Cornell University Press.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*(1), 5–25. doi:10.1111/j.1365-2575.2005.00183.x

Cavoukian, A. (2009). *Privacy by design... take the challenge*. *Communications of the ACM* (Vol. 53). Toronto, Canada: Office of the Information and Privacy Commissioner of Ontario. doi:10.1145/1743546.1743559

Charmaz, K. (2006). *Constructing grounded theory: a practical guide through qualitative analysis*. London; Thousand Oaks, Calif.: Sage Publications.

Checkland, P., & Scholes, J. (1990). *Soft systems methodology in action*. Chichester, West Sussex, England: Wiley.

Chuang, C. S. (2003). Human Rights concern in an Information Society: thoughts on personal Data Protection in Taiwan. *The World Summit on the Information Society-Asian Regional Conference*. Tokyo, Japan: World Summit on the Information Society. Retrieved from http://www.tahr.org.tw/site/english/wsis-chuang.htm

Clanchy, M. (1979). *From memory to written record: England 1066-1307*. London: Edward Arnold.

Cock, D., Wolf, C., & Preneel, B. (2006). The Belgian electronic Identity card overview. *Sicherheit*. Bonner KÄollen Verlag. Retrieved from http://www.cosic.esat.kuleuven.be/publications/article-769.pdf

Cock, D., Wouters, K., & Preneel, B. (2004). Introduction to the Belgian EID Card. *First European PKI Workshop: Research and Applications*, *3093*, 380. doi:10.1007/978-3-540-25980-0_1

Cofta, P. (2007). *Trust, Complexity and Control*. Chichester, UK: John Wiley & Sons. Retrieved from http://dx.doi.org/10.1002/9780470517857.fmatter

Cole, S. (2001). *Suspect identites*. Massachusetts: Harvard University Press.

Cole, S. (2004). Fingerprint identification and the criminal justice system: Historical lessons for the DNA debate. In D. Lazer (Ed.), *DNA and the criminal justice system: the technology of justice*. Cambridge, Mass.: MIT Press.

Collis, R. (2008). Concern voiced over drop in overseas visitors to the U.S. *The International Herald Tribune*. Retrieved from http://www.iht.com/articles/2008/03/05/travel/trfreq7.php

Colvin, M., & Spencer, M. (1995). *Identity cards revisited*. London, England: Institute of Public Policy Research.

Corbin, J. M., & Strauss, A. (1990). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications.

Dahl, S. (2004). Intercultural Research: the current state of knowledge. *Middlesex University Discussion Paper*, *26*. Retrieved from http://ssrn.com/paper=658202

Daston, L., & Galison, P. (1992). The Image of Objectivity. *Representations*, (40), 81–128. Retrieved from http://www.jstor.org/stable/2928741

Davies, S. (1999). *New techniques and technologies of surveillance in the workplace*. *MSF Information*.

Davis. (1983). *The return of Martin Guerre*. Cambridge, Mass.: Harvard University Press.

Davis. (1985). *A technology acceptance model for empirically testing new end-user information systems: theory and results*. Massachusetts Institute of Technology. Retrieved from http://dspace.mit.edu/handle/1721.1/15192

Davis, Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. doi:10.1287/mnsc.35.8.982

De Hert, P. (2007). *A right to identity to face the Internet of Things?* (pp. 1–21). Retrieved from http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de+Hert-Paul.pdf

DeCew, J. W. (1997). *In pursuit of privacy: law, ethics, and the rise of technology*. Ithaca, New York: Cornell University Press.

Denzin, N. K., & Lincoln, Y. S. (1998). *The landscape of qualitative research: theories and issues*. Thousand Oaks, Calif.: Sage Publications.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of management review*, *23*(3), 601–620. Retrieved from http://www.jstor.org/stable/259297

Dunleavy, P. (2006). *Digital era governance: IT corporations, the state, and E-government*. Oxford, UK: Oxford University Press. Retrieved from http://eprints.lse.ac.uk/id/eprint/12222

EPIC. (2007). *United States Visitor and Immigrant Status Indicator Technology*. Retrieved from http://epic.org/privacy/us-visit/

Elliot, R. (2006). An early experiment in National Identity Cards: the battle over registration in the First World War. *Twentieth Century British History*, *17*(2), 145–176. doi:doi:10.1093/tcbh/hwl006

Eltis, D. (2002). *Coerced and free migration: global perspectives*. Stanford, Calif.: Stanford University Press.

European Commission Home Affairs. (2010). Schengen area. Retrieved December 21, 2010, from http://ec.europa.eu/home-affairs/policies/borders/borders_schengen_en.htm

Every Child Matters. (2007). *ICS, CAF and ContactPoint: an overview*. Every Child Matters. Retrieved from http://www.everychildmatters.gov.uk/_files/ICS CAF and ContactPoint overview Nov 2007.pdf

Federal Trade Commission. (1998). Fair information practice principles. Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Field, A. (2009). *Discovering statistics using SPSS*. Los Angeles, California: Sage Publications.

Finlay, R. (1988). The Refashioning of Martin Guerre. *The American Historical Review*, *93*(3), 553–571. Retrieved from http://www.jstor.org/stable/1868102

Finn, J. (2005). Photographing fingerprints: data collection and state surveillance. *Surveillance & Society*, *3*(1), 21–44.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: an introduction to theory and research. Reading, Massachusetts: Addison-Wesley.

Flaherty, D. (1979). *Privacy and government data banks: an international perspective*. London: Mansell.

Flick, U. (2002). *An introduction to qualitative research*. Sage Publications.

Flick, U. (2007). *Managing quality in qualitative research*. Los Angeles: Sage Publications.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*(2), 219–245. doi:10.1177/1077800405284363

Fontana, J. (2003). *A National Identity card for Canada?* Candada. Retrieved from http://www.oipc.bc.ca/pdfs/public/cimmrp06-e.pdf

Fosdick, R. (1915). Passing of the Bertillon system of identification. *Journal of Criminal Law and Criminology*, *6*, 363.

Fussell. (2004). Genocide and group classification on National ID cards. In C. Watner & W. McElroy (Eds.), *National identification systems : essays in opposition*. Jefferson: McFarland.

Garcelon. (2001). Colonizing the subject: the genealogy and legacy of the soviet internal passport. In J. Caplan & J. C. Torpey (Eds.), *Documenting individual identity : the development of state practices in the modern world*. Princeton, N.J.: Princeton University Press.

Garfinkel, S. (2001). *Database nation: the death of privacy in the 21st century*. O'Reilly.

Garfinkel, S., Margrave, D., Schiller, J. I., Nordlander, E., & Miller, R. C. (2005). How to make secure email easier to use. *SIGCHI conference on Human factors in computing systems* (pp. 701–710). Portland, Oregon, {USA}: ACM. doi:10.1145/1054972.1055069

Gibson, M. (2002). *Born to crime: Cesare Lombroso and the origins of biological criminology*. Westport: Praeger.

Giddens, A. (1991). *The Consequences of Modernity* (1st ed.). Stanford University Press.

Gordon, L., & Loeb, M. (2006). *Managing cybersecurity resources: a cost-benefit analysis*. New York: McGraw-Hill.

Graham, E. (2007). DNA reviews: the national DNA database of the United Kingdom. *Forensic Science, Medicine, and Pathology*, *3*(4), 285–288. doi:10.1007/s12024-007-9014-8

Groebner, V. (1999). Inside Out: clothes, dissimulation, and the arts of accounting in the autobiography of Matthaeus Schwarz, 1496-1574. *REPRESENTATIONS*, (66), 100–121.

Groebner, V. (2001). Describing the person, reading the signs in late medieval and reanaissance Europe: identity papers, vested figures, and the limits of identification, 1400 - 1600. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey 08540: Princeton University Press.

Grommen, S. (2009, September 9). 1 op 5 gebruikt eID op het werk. *Data News*. Retrieved from http://datanews.knack.be/ict/nieuws/nieuwsoverzicht/2009/09/08/1-op-5-gebruikt-eid-op-het-werk/article-1194716226507.htm

Gutwirth, S. (2009). Beyond identity? *Identity in the Information Society*, *1*(1), 123–133. doi:10.1007/s12394-009-0009-3

Gürses, S. (2010). PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity in the Information Society*, *3*(3), 539–563. doi:10.1007/s12394-010-0073-8

Hall, E. T. (1984). *The dance of life: the other dimension of time*. Anchor.

Halperin, R., & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society*, *1*(1), 71–87. doi:10.1007/s12394-008-0004-0

Halperin, R., & Backhouse, J. (2012). Risk, trust and eID: Exploring public perceptions of digital identity systems. *First Monday*, *17*(4). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3867

Hansen, M., Pfitzmann, A., & Steinbrecher, S. (2008). Identity management throughout ones whole life. *Information Security Technical Report*, *13*(2), 83–94. doi:10.1016/j.istr.2008.06.003

Hemant, K., Srikanth, N., & Sanjay, S. (2010). *A UID numbering scheme*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189

Henry, J. (2008, November 13). National database will not stop deaths like Baby P. *Telegraph*. Retrieved from http://blogs.telegraph.co.uk/julie_henry/blog/2008/11/13/national_database_will_not_stop_deaths_like_baby_p

Hickson, D., & Pugh, D. (1995). *Management worldwide: the impact of societal culture on organizations around the globe*. Penguin.

Hildebrandt, M. (2008). Profiling and the rule of law. *Identity in the Information Society*, *1*(1), 55–70. doi:10.1007/s12394-008-0003-1

Hindle, S. (2004). Dependency, shame and belonging: badging the deserving Poor, c.1550-1750. *Cultural and Social History*, *1*, 6–35. doi:10.1191/1478003804cs0003oa

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2009). Privacy as information access and illusory control: The case of the facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1). doi:10.1016/j.elerap.2009.05.001

Hofstede. (2001). *Cultures Consequences: Comparing Values, Behaviors, Institutions, and Organisations across nations*. SAGE. Retrieved from http://books.google.com/books?id=w6z18LJ_1VsC&printsec=frontcover&dq=cultures+consequences&lr=#PPR17,M1

Hofstede. (2005). *Cultures and Organizations: Software for the Mind*. McGraw-Hill.

Hofstede, G, & Bond, M. (1988). The Confucius connection: From cultural roots to economic growth. *Organizational dynamics*. Retrieved from http://www2.seminolestate.edu/falbritton/Summer 2009/FHI/Articles/Hofstede.confucious connection 120505 science direct.pdf

Hofstede, Geert, Minkov, M., & Vinken, H. (2008, January). Value Survey Module 2008 manual. Retrieved from http://feweb.uvt.nl/center/hofstede/VSMChoice.html

Home Office. (2005). *Identity Cards benefits overview*.

Home Office Identity Documents Bill 2010-11 (2010). London, England: House of Commons. Retrieved from http://services.parliament.uk/bills/2010-11/identitydocuments.html

House of Lords Data Protection Act 1998 (1998). London, England: House of Lords.

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human-Computer Interaction*, *1*(1), 1–137. doi:10.1561/1100000004

Identity Cards Act (2006). London, England: House of Lords. Retrieved from http://www.legislation.gov.uk/ukpga/2006/15/contents

Identity Fraud Steering Committee. (2006). New estimate of cost of Identity Fraud to the UK economy. *Home Office*. London, England: Home Office.

Identity and Passport Service. (2006). *Strategic action plan for the National Identity Scheme*. London, England. Retrieved from http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/976.htm

Identity and Passport Service. (2008). *National Identity Scheme Delivery Plan 2008: a response to consultation*. London, England. Retrieved from http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/956.htm

Identity and Passport Service. (2009). *National Identity Service: delivery update 2009*. London, England. Retrieved from http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1052.htm

Identity and Passport Service. (2010). *Annual report and accounts 2009-2010*. London, England. Retrieved from http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1717.htm?advanced=&searchoperator=&searchmodifier=&verb=&search_date_from=&search_date_to=&stage=&search_event_subject=&search_category=&search_query=&search_scope=&search_group=&varChunk=

Indigov. (2009). *Belgen verdeeld over gebruik van eID op het werk*. Brussels.

Institute for Public Policy Research. (1995). *Identity cards: revisited*. London: Justice.

Isikoff, M., & Pape, E. (2004, May). Exclusive: Mysterious Fingerprint. *Newsweek*. Retrieved from http://www.thedailybeast.com/newsweek/2004/05/30/exclusive-mysterious-fingerprint.html

Joseph, A. (2001). Anthropometry, the police expert and the deptford murders: The contested introduction of fingerprinting for the identification of criminals in late Victorian and Edwardian Britain. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618–644. doi:10.1016/j.dss.2005.05.019

Jøsang, A., & Pope, S. (2005). User-Centric Identity Management. *Asia Pacific Information Technology Security Conference* (Vol. 5). doi:10.1109/MSP.2007.99

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and privacy in identity management architectures. *Fifth Australasian symposium on ACSW frontiers* (pp. 143–152). Darlinghurst, Australia: Australian Computer Society. Retrieved from http://portal.acm.org/citation.cfm?id=1274548

Kabatoff, M., & Daugman, J. (2008). Pattern Recognition: Biometrics, Identity and the State? An Interview with John Daugman. *Biosocieties*, *3*(01), 81–86. doi:10.1017/S1745855208005966

Kaluszynski, M. (2001). Republican identity: Bertillonage as a government technique. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Kempner, R. (1946). The German National Registration System as means of police control of population. *Journal of Criminal Law and Criminology (1931-1951)*, *36*(5), 362–387. Retrieved from http://www.jstor.org/stable/1138058

Kent, S., & Millett, L. (2002). *IDs? Not that easy: questions about nationwide Identity Systems*. Washington, United States: National Academies Press. doi:10.1016/j.jgi.2003.12.017

Kim, D., Ferrin, D., & Rao, H. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. doi:10.1016/j.dss.2007.07.001

King, G., Keohane, R., & Verba, S. (1994). *Designing social inquiry*. Princeton, N.J.: Princeton University Press.

Kitzinger, J., & Barbour, R. S. (1999). *Developing focus group research: politics, theory, and practice*. London; Thousand Oaks: Sage Publications.

Kroeber, A., & Kluckhohn, C. (1963). *Culture: a critical review of concepts and definitions*. New York: Vintage Books.

Krueger, R., & Casey, M. (2000). *Focus groups: a practical guide for applied research*. Thousand Oaks, California: Sage Publications.

Kubicek, H. (2010). Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. *Identity in the Information Society*, *3*(1), 5–26. doi:10.1007/s12394-010-0052-0

Kubicek, H., & Noack, T. (2010a). The path dependency of national electronic identities. *Identity in the Information Society*, *3*(1), 111–153. doi:10.1007/s12394-010-0050-2

Kubicek, H., & Noack, T. (2010b). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society*, *3*(1), 235–245. doi:10.1007/s12394-010-0063-x

Laming, H. (2003). *The Victoria Climbié inquiry: report of an inquiry*. London: Stationery Office.

Layne, K., & Lee, J. (2001). Developing fully functional e-government: a four stage model. *Government Information Quarterly*, *18*(2), 122–136. doi:10.1016/S0740-624X(01)00066-1

Lee, H., & Gaensslen, R. (1991). *Advances in fingerprint technology*. New York: CRC Press.

Leitold, H., & Posch, K. (2004). Austria citizen card: a bottom up view. In B. Jerman-Blažič, W. Schneider, & T. Klobučar (Eds.), *Security and privacy in advanced networking technologies* (p. 247). Oxford, UK: North Atlantic Treaty Organisation.

Lettice, J. (2005, December 1). EU ministers approve biometric ID, fingerprint data sharing. *The Register*. Retrieved from http://www.theregister.co.uk/2005/12/01/jahc_biometric_id_standards/

Lettice, J. (2007, June 22). UK Gov seeks "scientific" basis for nationality. *The Register*. Retrieved from http://www.theregister.co.uk/2007/06/22/triesman_scientific_id/

Li, X. (2004). *Trust in national identification systems: a trust model based on the TRA/TPB*. Washington State University.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, Calif.: Sage Publications.

Lips, M. (2007). E-Government under construction: challenging traditional conceptions of citizenship. In P. G. Nixon & V. N. Koutrakou (Eds.), *E-government in Europe: re-booting the State*. London: Routledge.

Lips, M., Taylor, J., & Organ, J. (2005). Electronic government: towards new forms of authentication, citizenship and governance. *Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities*. Oxford, UK: Oxford Internet Business School.

Lips, Taylor, J., Organ, J., Bekkers, V., van Duivenboden, H. P. M., & Thaens, M. (2006). Identity Management as public innovation: looking beyond ID cards and authentication systems. *{ICT} and Public Innovation: assessing the modernisation of public administration*. {IOS} Press. Retrieved from http://en.scientificcommons.org/23571231

LoBaido, A. (2000, July 11). Greek Christians battle over ID cards. *World Net Daily*. Retrieved from http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=19088

Lombroso, C., & Horton, H. P. (1911). *Crime, its causes and remedies*. Montclair, NJ: Patterson Smith.

London School of Economics. (2005). *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*. London, England. Retrieved from http://identityproject.lse.ac.uk/

Lucassen, L. (1998). The Great War and the end of free migration in Western Europe and United States: explanations and refutations. In A. Böcker (Ed.), *Regulation of migration: international experiences*. Amsterdam: Het Spinhuis.

Lucassen, L. (2001). A many-headed monster: The evolution of the passport system in the Netherlands and Germany in the long nineteenth ceentury. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Luhmann, N. (1979). *Trust and power*. Chichester, UK: John Wiley & Sons.

Lunt, P., & Livingstone, S. (1996). Rethinking the focus group in media and communications research. *Journal of communication*, *46*(2), 79–98. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.1996.tb01475.x/abstract

Lusoli, W., Maghiros, I., & Bacigalupo, M. (2009). eID policy in a turbulent environment: is there a need for a new regulatory framework? *Identity in the Information Society*, *1*(1), 173–187. doi:10.1007/s12394-009-0011-9

Lyon, D. (2002). *Surveillance society: monitoring everyday life*. Buckingham, Philadelphia: Open University Press.

Lyon, D. (2005). *Surveillance society: monitoring everyday life*. Buckingham, Philadelphia: Open University Press. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Surveillance+society+:+monitoring+everyday+life#0

Lyon, D. (2007). National ID cards: crime-control, citizenship and social sorting. *Policing*, *1*(1), 111–118. doi:10.1093/police/pam015

Lyon, D. (2009). *Identifying citizens: ID cards as surveillance*. Cambridge, UK: Polity.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. doi:10.1287/isre.1040.0032

Mariën, I., & Audenhove, L. (2010). The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society*, *3*(1), 27–41. doi:10.1007/s12394-010-0042-2

Marks, D., & Yardley, L. (2004). *Research methods for clinical and health psychology*. Thousand Oaks, California: Sage Publications.

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, *3*(1), 213–233. doi:10.1007/s12394-010-0044-0

Matthews, M. (1993). *The passport society: controlling movement in Russia and the USSR*. Boulder, Colorado: Westview Press.

Mayer, R. C., Davis, J. H., & Schoorman, F. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709–734. Retrieved from http://www.jstor.org/stable/258792

Mayer-Schönberger, V. (2009). Delete: the virtue of forgetting in the digital age. Princeton, N.J.: Princeton University Press.

Mayer-Schönberger, V. (1997). Generational development of data protection in Europe. In P. Agre & M. Rotenberg (Eds.), *Technology and privacy: the new landscape* (pp. 219–241). Cambridge, MA, USA: MIT Press. Retrieved from http://portal.acm.org/citation.cfm?id=275283.275292

McCarthy, J., & Wright, P. (2004). Technology as experience. *interactions*, *11*(5), 42–43. doi:10.1145/1015530.1015549

McKnight, D., & Chervany, N. (2001). Conceptualizing trust: a typology and e-commerce customer relationships model. *System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on* (p. 10 pp.).

McKnight, D., Choudhury, V., & Kacmar, C. (2002a). Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research*, *13*(3), 334–359. doi:10.1287/isre.13.3.334.81

McKnight, D., Choudhury, V., & Kacmar, C. (2002b). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, *11*(3-4), 297–323. doi:10.1016/S0963-8687(02)00020-3

McSweeney, B. (2002). Hofstede's model of national cultural differences and their consequences: a triumph of faith - a failure of analysis. *Human Relations*, *55*(1), 89–118. doi:10.1177/0018726702551004

Mcknight, D., Cummings, L., & Chervany, N. (1998). Initial Trust Formation in new organizational relationships. *Academy of management review*, *23*(3), 473–490.

Meints, M., & Hansen, M. (2006). *Study on ID documents*. Retrieved from http://www.fidis.net/resources/deliverables/hightechid/int-d36000/doc/1/

Mentis, M., & Zwingelbery, H. (2009). *Identity Management Systems - recent developments*. Retrieved from http://www.fidis.net/resources/deliverables/profiling/#c1764

Milberg, S., Burke, S., Smith, & Kallman, E. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65–74. doi:10.1145/219663.219683

Milberg, S., Smith, & Burke, S. (2000). Information Privacy: corporate management and national regulation. *Organization Science*, *11*(1), 35–57. Retrieved from http://www.jstor.org/stable/2640404

Morgan, David. (1996). Focus Groups. *Annual Review*, *22*, 33:259–54. Retrieved from http://www.jstor.org/discover/10.2307/2083427?uid=3739256&uid=2134&uid=2&uid=70&uid=4&sid=21101206628227

Morgan, David. (2006, November 30). Border security system posts just 1 terror case. *Reuters*. Washington, United States. Retrieved from http://uk.reuters.com/article/2006/11/30/us-security-usa-fingerprints-idUKN2938529920061130

Morgan, De. (2009, September 7). Meer dan helft Belgische werknemers wantrouwt eID-kaart. *De Standaard*. Retrieved from http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20090907_023

Munro, E. (2008). Eileen Munro: Lessons learnt, boxes ticked, families ignored. *The Independent*. Retrieved from http://www.independent.co.uk/opinion/commentators/eileen-munro-lessons-learnt-boxes-ticked-families-ignored-1020508.html

Murr, A. (2004, June). The wrong man. *Newsweek*.

Murray, J. (2008, September 2). Database delayed: critics fear children may be in danger. *The Guardian*. Retrieved from http://www.guardian.co.uk/education/2008/sep/02/schools.children1

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. Retrieved from http://heinonline.org/HOL/Page?handle=hein.journals/washhlr79&id=129&div=&collection=journals

Noack, T., & Kubicek, H. (2010). The introduction of online authentication as part of the new electronic national identity card in Germany. *Identity in the Information Society*, *3*(1), 87–110. doi:10.1007/s12394-010-0051-1

Noiriel, G., & Laforcade, G. (1996). *The French melting pot*. Minneapolis: University of Minnesota Press.

Paine, C., Reips, U., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users perceptions of “privacy concerns” and “privacy actions.” *International Journal of HumanComputer Studies*, *65*, 526536. doi:10.1016/j.ijhcs.2006.12.001

Palen, L., & Dourish, P. (2003). Unpacking “privacy” for a networked world. *CHI’03: Conference on Human factors in computing systems* (p. 129–136). New York: ACM. doi:10.1145/642611.642635

Papademetriou, D. G. (2005, September). The global struggle with illegal migration: no end in sight. *Migration Policy Institue*. Migration Policy Institute. Retrieved from http://www.migrationinformation.org/Feature/display.cfm?id=336

Parliamentary Office of Science and Technology. (2006). *The national DNA database*. Retrieved from http://www.parliament.uk/documents/upload/postpn258.pdf

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). London: Sage Publications.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134. Retrieved from http://mesharpe.metapress.com/index/ymy1p2ngk06wt39f.pdf

Pfitzmann, A., & Hansen, M. (2008, February). Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – a consolidated proposal for terminology. Retrieved from http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Identity*. Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Pfitzmann, K., Hansen, M., Liesebach, K., Pfitzmann, A., & Steinbrecher, S. (2006). What user-controlled identity management should learn from communities. *Information Security Technical Report*, *11*(3), 119–128. doi:10.1016/j.istr.2006.03.008

Pollitt, C. (2003). Joined-up Government: a Survey. *Political Studies Review*, *1*(1), 34–49. doi:10.1111/1478-9299.00004

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: a practical model for user control of privacy. *International Journal of HumanComputer Studies*, *63*, 228253. doi:http://dx.doi.org/10.1016/j.ijhcs.2005.04.008

Privacy International. (2004). *The enhanced US border surveillance system: an assessment of the implications of US-VISIT*. Retrieved from http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf

Punch, K. (1998). *Introduction to social research: quantitative and qualitative approaches*. Sage Publications.

Rahaman, A., & Sasse, M. A. (2011). A framework for the lived experience of identity. *Identity in the Information Society*, *3*(3), 605–638. doi:10.1007/s12394-010-0078-3

Rayner, G., Gammell, C., & Britten, N. (2008). Madeleine McCann DNA "an accurate match." *Telegraph.co.uk*. Retrieved from http://www.telegraph.co.uk/news/worldnews/1562710/Madeleine-McCann-DNA-an-accurate-match.html

Razak, A. (2007). Brunei , M ' sia first in SEA to use IC as passport. *Brunei Times*. Retrieved from http://www.bt.com.bn/news/2007/08/16/brunei_msia_first_in_sea_to_use_ic_as_passport

Resnick, P., & Varian, H. R. (1997). Recommender systems. *Communications of the ACM*, *40*(3), 58. doi:10.1145/245108.245121

Riegelsberger, J., Sasse, M. A., & Mccarthy, J. D. (2005). The mechanics of trust: a framework for research and design. *International Journal of Human-Computer Studies*, *62*(3), 381–422. doi:10.1016/j.ijhcs.2005.01.001

Rosenzwig, P., Kochems, A., & Schwartz, A. (2004). *Biometric Technologies: Security, Legal, and Policy Implications*. *Legal Memorandum*. Retrieved from http://www.heritage.org/Research/HomelandSecurity/lm12.cfm

Ruggiero, K. (2001). Fingerprinting and the Argentine plan for universal identification in the late nineteenth and early twentieth centuries. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Said Ya'akub, I. (2007). Brunei , Malaysia first in Asean to implement FTC. *Brunei Times*. Retrieved from http://www.bt.com.bn/news/2007/09/11/brunei_malaysia_first_in_asean_to_implement_ftc

San Antonio Express. (2008, February). Leaders along border fear US-VISITs impact. *San Antonio Express*. Retrieved from http://www.mysanantonio.com/news/MYSA23_03A_Border_Trade_323_118705ca_html29416.html

Sankar, P. (2001). DNA-Typing: Galton's eugenic dream realized? In J. Caplan & J. C. Torpey (Eds.), *Documenting individual identity: the development of state practices in the modern world*. New Jersey: Princeton University Press.

Sasse, M. A. (1997). *Eliciting and describing users' models of computer systems*. University of Birmingham.

Schafer, J. B., Konstan, J. A., & Riedl, J. (2001). E-commerce recommendation applications. *Data mining and knowledge discovery*, *5*(1), 115–153. doi:10.1023/A:1009804230409

Schneier, B. (2003). *Beyond fear: thinking sensibly about security in an uncertain world*. New York: Copernicus Books. Retrieved from http://books.google.co.uk/books?hl=en&lr=&id=wuNImmQufGsC&oi=fnd&pg=PA1&ots=8UfgjuDz8B&sig=PSU78EmTc0d22pVLrj5Szqt8fd4#v=onepage&q&f=false

Schwartz, S. H. (1999). A theory of cultural values and some implications for work. *Applied Psychology*, *48*(1), 23–47. doi:10.1111/j.1464-0597.1999.tb00047.x

Scott, J. C. (1998). *Seeing like a state: how certain schemes to improve the human condition have failed*. New Haven: Yale University Press.

Seale, C. (1999). *The quality of qualitative research*. London; Thousand Oaks, Calif.: Sage Publications.

Senicar, V., Jerman-Blazic, B., & Klobucar, T. (2003). Privacy-Enhancing Technologies: approaches and development. *Computer Standards & Interfaces*, *25*(2), 147–158. doi:10.1016/S0920-5489(03)00003-5

Shiels, M. (2010). Gamers ' victory over real names. *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/technology/8806623.stm

Silcock, R. (2001). What is E-government. *Parliamentary Affairs*, *54*(1), 88–101. doi:10.1093/pa/54.1.88

Silverman, D. (2004). *Qualitative research: theory, method and practice*. London: Sage Publications.

Smith. (1993). Privacy policies and practices: inside the organizational maze. *Communications of the ACM*, *36*(12), 104122. doi:10.1145/163298.163349

Smith, I., LaMarca, A., Consolvo, S., & Dourish, P. (2004). A social approach to privacy in location enhanced computing. *The Kluwer International Series in Engineering and Computer Science*, *780*(IV), 157–167. doi:10.1007/0-387-23462-4_17

Smith, Milberg, S. J., & Burke, S. J. (1996). Information Privacy: measuring individuals concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. Retrieved from http://www.jstor.org/stable/249477

Sokolov, D. (2006a, January 27). Österreichs größtem Signatur-Anbieter droht die Pleite. *Heise Online*. Retrieved from http://www.heise.de/newsticker/meldung/68944&sl=de&tl=en

Sokolov, D. (2006b, February 7). Österreichs signaturanbieter A-Trust sucht den weg aus der krise. *Heise Online*. Retrieved from http://www.heise.de/newsticker/Oesterreichs-Signaturanbieter-A-Trust-sucht-den-Weg-aus-der-Krise--/meldung/69316

Sondergaard, M. (1994). Hofstedes consequences: a study of reviews, citations and replications. *Organization Studies*, *15*(3), 447–456. doi:10.1177/017084069401500307

Spencer-Oatey, H. (2008). *Culturally speaking: culture, communication and politeness theory*. London: Continuum.

Steinwedel, C. (2001). Making social groups, one person at a time: identification of individuals by estate, religious confession, and ethnicity in late imperial Russia. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Strauss, A., & Corbin, J. M. (1998). *Basics of qualitative research techniques and procedures for developing grounded theory*. Thousand Oaks: Sage Publications. Retrieved from http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=63250

Tanner, L. (2007). *Labor delivers on savings*. *Media*. Canberra, Australia: Parliment of Australia. Retrieved from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=(Id:media/pressrel/dm0p6);rec=0;

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: combining qualitative and quantitative approaches*. Thousand Oaks, California: Sage Publications.

Taylor, J., Lips, M., & Organ, J. (2006). *The citizen, the state and the ID nexus: attention to information, societal shaping and modes of citizen sorting*. York.

Taylor, R. N., & Coutaz, J. (1994). Software Engineering And Human-Computer Interaction. *Icse '94 Workshop On Se-Hci: Joint Research Issues*. Sorrento, Italy: Springer.

The European Court of Human Rights. (2008). *Case of S. and Marper v. the United Kingdom*. Strasbourg: European Court of Human Rights. Retrieved from http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=DNA&sessionid=86680546&skin=hudoc-en

The Independent. (2007, September 16). The McCanns: unbelievable truth or unimaginable nightmare? *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/the-mccanns-unbelievable-truth-or-unimaginable-nightmare-402486.html

Thompson, W., Taroni, F., & Aitken, C. (2003). How the probability of a false positive affects the value of DNA evidence. *Journal of Forensic Sciences*, *48*(1), 47–54. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/12570198

Tony Blair. (1999). *Modernising government*. *Financial Accountability & Management*. London, England: Wiley Online Library. Retrieved from http://www.archive.official-documents.co.uk/document/cm43/4310/4310-00.htm

Torpey, J. (2000). *The invention of the passport: surveliiance, citizenship and the state*. Cambridge: Cambridge University Press.

Torpey, J. (2001). The Great War and the birth of the modern passport system. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. New Jersey: Princeton University Press.

Triandis, H. (1972). *The analysis of subjective culture*. New York: John Wiley & Sons.

Trompenaars, A., & Hampden-Turner, C. (1994). *Riding the Waves of Culture: Understanding Diversity in Global Business*. McGraw-Hill.

Turow, J., King, J., Hoofnagle, C., Bleakley, A., & Hennessy, M. (2005). *Americans reject tailored advertising and three activities that enable It*. *SSRN eLibrary*. Retrieved from http://ssrn.com/abstract=1478214

U.S. Senate Enhanced border security and visa entry reform act of 2002 (2002). Washington, United States of America: House of Senate. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ173/content-detail.html

UCL Registry & Academic evices. (2012). Undergraduate Student Numbers by Faculty and Year Group 2011-12. Retrieved September 9, 2012, from http://www.ucl.ac.uk/ras/statistics/current/B

UK Border Agency. (2012). Registering for IRIS. Retrieved February 1, 2012, from http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/registeriris/

Unique Identification Authority of India. (2009). *Biometric design standards for UID applications*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189#docs

Unique Identification Authority of India. (2010a). *UIDAI strategy overview: creating a unique identity number for every resident in India*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189#docs

Unique Identification Authority of India. (2010b). *Aadhaar handbook for registrars*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189#docs

Unique Identification Authority of India. (2010c). *UID and NREGA*. India. Retrieved from http://uidai.gov.in/index.php?option=com_content&view=article&id=149&Itemid=189#docs

Unique Identification Authority of India. (2010d). Envisioning a role for Aadhaar in the Public Distribution System. India.

Varney, S. D. (2006). *Service transformation: a better service for citizens and businesses, a better deal for the tax payer*. Norwich. Retrieved from http://www.official-documents.gov.uk/document/other/011840489X/011840489X.pdf

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh, V., & Davis, F. D. (2010). Theoretical acceptance extension model: field four studies of the technology longitudinal. *Management Science*, *46*(2), 186–204. Retrieved from http://www.jstor.org/stable/2634758

Wallace, H. (2006). The UK national DNA database: balancing crime detection, human rights and privacy. *EMBO Reports*, *7*(SI), S26–S30. doi:10.1038/sj.embor.7400727

Wallerstein, I. (1990). Culture as the ideological battleground of the modern world-system. *Theory Culture Society*, *7*(2), 31–55. doi:10.1177/026327690007002003

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets*, *12*(3), 157–162. doi:10.1080/101967802320245929

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220. Retrieved from http://www.jstor.org/stable/1321160

Waters, D. (2009). EC starts legal action over Phorm. *BBC News*, pp. 14–15. London, England. Retrieved from http://news.bbc.co.uk/1/hi/7998009.stm

Weber, M., Roth, G., & Wittich, C. (1978). *Economy and society: an outline of interpretive sociology*. Berkeley: University of California Press.

Weirich, D. (2001). Persuasive password security. *CHI'01 extended abstracts on Human factors in* (pp. 1–2). New York, NY, USA: ACM. doi:10.1145/634067.634152

Weirich, D. (2005). *Persuasive password security*. *CHI'01 extended abstracts on Human factors in*. University College London.

Werth, N. (2004). The Russian card: the Propiska. In C. Watner & W. McElroy (Eds.), *National identification systems: essays in opposition*. Jefferson: McFarland.

White, P. (2008). *Managing enterprise complexity: the use of Identity Management Architecture to control enterprise resources*. Charles Sturt University.

Whitefield, A., Wilson, F., & Dowell, J. (1991). A framework for human-factors evaluation. *Behaviour Information Technology*, *10*(1), 65–79. Retrieved from http://discovery.ucl.ac.uk/143209/

Whitley, E. a., & Hosein, G. (2010). Global identity policies and technology: do we understand the question? *Global Policy*, *1*(2), 209–215. doi:10.1111/j.1758-5899.2010.00028.x

Windley, P. J. (2005). *Digital identity*. Sebastopol, California: O'Reilly.

Woodbridge, J. (2005). *Sizing the unauthorised (illegal) migrant population in the United Kingdom in 2001*. *Home Office*. London, England: Home Office. Retrieved from http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr2905.pdf

Wray, R. (2009, April 14). Phorm: UK faces court for failing to enforce EU privacy laws. *Guardian*. London. Retrieved from http://www.guardian.co.uk/business/2009/apr/14/phorm-privacy-data-protection-eu

Yates, F. A. (1966). *The art of memory*. Chicago: University of Chicago Press.

Yunos, R. (2009, February 1). Immigration services through the ages. *Brunei Times*. Retrieved from http://www.bt.com.bn/golden_legacy/2009/02/01/immigration_services_through_the_ages

Appendix II: Individual Study – Focus Group Scenarios

Scenario 1
The government is concerned about the safety of children. As such, the government wants several different agencies to work together to ensure the safety of children.

Solution
The government aims to encourage data sharing by creating a comprehensive database that is accessible across different private and public organizations. All careers (teachers, doctors, police officers, etc.) that come into contact with a child can insert records or comments on their encounter with the child. These careers also have access to other comments or records, inserted by other careers, in relation to that particular child.

Use Case Example
Junior (child) is being treated by Jane (doctor) for recent injuries
1. Jane suspects this is a case of child abuse
2. Jane access Junior's record on the system
3. Jane inserts a note of her suspicion along with medical records
4. Jane reviews other notes on Junior made by other careers
5. Jane does not find any strong evidence to prove abuse and discharges Junior

John (teacher) is concerned about Junior exhibiting worrying behaviour
1. John access Junior's record on the system
2. John makes a note of his concerns
3. John reviews other notes of Junior made by other careers
4. John comes across Jane's note of potential abuse
5. John thinks that this explains Junior's behaviour
6. John notifies the proper authorities, which then investigate the situation and the parents

Potential Extension
The police are interested in using the health department system to track delinquent behaviour. They believe that early signs of troubled behaviour may eventually lead to a life of crime. In using so, they aim to access child records to keep a close watch on children who exhibit certain behaviour.

Scenario 2
The government is concerned about the level ofpersonal debt that citizens carry. It has concluded that many people are living beyond their means, are in debt and are dependent on loans.

Solution
The government aims to regulate the application of loans by capping the amount that people can borrow. In order to do so, the government intends to pull information from stores and different financial institutions like banks and insurance companies. In doing so, the bank can monitor spending and saving habits of citizens which will affect the amount that can be borrowed.

Use Case
John goes to a bank to apply for a loan for a certain amount
1. John fills in a loan application, specifying the amount and hands it to the bank clerk
2. The clerk forwards John's application details to the government system
3. The government system then pulls information all of John's various bank accounts to monitor his saving habits.
4. The government system then pulls information from all stores about John's purchasing habits.
5. The government system then uses this information to calculate a risk profile
6. The system uses the risk profile to determine that John cannot get a loan for the amount requested because he is unlikely to able to pay back the debt
7. The system forwards the information to the bank
8. The bank denies John's application

Possible Extension
The government is interested in extending the system to provide individuals with advice to change spending and saving habits. This would help to ensure that he is eventually capable of getting a loan for the amount needed. Another possible extension is to work closely with stores to dynamically change the pricing of certain goods depending on the individual's profile. It is hoped that this will deter individuals from spending money on goods they don't need reducing the chances of going into debt.

Scenario 3
Health agencies are concerned about the growing problem of obesity. It is a problem that puts individuals at great risk and is becoming a burden on the medical system.

Solution
The health department has proposed to set up a monitoring program that is compulsory for everyone. Under this scheme the health department will have a centralized database that will store all medical records. Additionally, the system will track individual food habits and exercise habits using CCTV (security cameras) and face recognition. All individuals will need to register by providing a digital photograph that can be used for facial recognition.

3.2 Use case
Jane purchases food products from a store
1. All store counters have CCTV cameras recording at all times
2. Jane goes to counter and presents her goods for purchase
3. The CCTV system records everything
4. Jane pays for her goods
5. The store forwards its CCTV footage to health department
6. At the health department, the video passes through facial recognition system
7. The system identifies Jane
8. The system analyzes the video to identify the goods that Jane purchased
9. All purchased goods and the video feed are stored on the database

Jane goes to the gym to exercise
1. All gyms have CCTV cameras recording the workout area at all times
2. Jane enters the gym
3. Jane performs her workout
4. Jane leaves the gym
5. The gym forwards its CCTV footage to the health department
6. At the health department, the video passes through facial recognition system
7. The system identifies Jane
8. The analyzes the video to track Jane's physical activity
9. The level of activity and the video feed are stored on the database

Identifying Jane at risk for obesity
1. The health department goes through each record in the database
2. Individuals whose food purchasing habits might lead to obesity are marked
3. Jane has been marked
4. The health department goes through Jane's activity level
5. The department thinks that Jane isn't doing enough
6. The department calls Jane in for a check up and to give Jane advice

3.3 Potential Extension
The government believes that it spends a major part of its budget on obesity related conditions. Therefore, using the system the government would like to charge those who do not follow the advice given with higher medical charges.

Another possible extension is to use the video footage to track behaviour or moods of individuals. Any behaviour that is out of the normal pattern for each individual alerts the health department of possible mental disorders or breakdowns. This will is believed to help control and keep an eye on potentially unstable individuals.

Scenario 4
The government is concerned about the rise of benefit fraud (falsely claiming financial support from the government). The welfare department in charge of the benefits believes that this is likely due to people providing false information and intends to claim benefit for life.

Solution The welfare department proposes a solution that makes use of biometrics (fingerprint, iris, etc.) together with a central database connected to other relevant public or private bodies. In order for the system to work, all citizens will be enrolled into the system even if they do not claim any benefits

Use Case
John is unemployed and applies for work (unsuccessfully)
1. The employer identifies John using a fingerprint system
2. The employer makes notes on John's application (job type, suitability, John's appearance, John's commitment to the process etc.)
3. The employer forwards all this information including the fingerprint through a network to the welfare department for storage in the database
4. John doesn't get the job
5. The employer forwards this information to the welfare department for storage.

John claiming for unemployment benefits
1. John goes to the welfare department to make a claim
2. John is asked to present his fingerprint
3. The system reads John's fingerprint and pulls all of John's records stored in the database
4. The welfare department looks at John's records and decides if John is actively trying to improve his situation where possible
5. Welfare department decides if John should get benefits

Possible Extension
The welfare department is interested in introducing a tiered scheme of benefits. Those who appear to be sincere in improving their situation will receive more benefits than those who show less initiative.

Scenario 5
The police are concerned about the rising levels of crime in the country. As a result the government hopes to make it harder for criminals to escape conviction by implementing a robust identification system.

Solution
The authorities aim to make use of a DNA database to quickly identify criminals. Under this scheme, DNA samples will be collected and stored from all suspects. The police will retain DNA from all suspects including ones that have not be proven to be guilty.

Use Case
Collecting DNA from suspects of a crime
1. Police identify John and Jane, among others, as a suspect of the crime
2. Officers confront John and collect his DNA information
3. Officers confront Jane and collect her DNA information
4. Officers collect DNA information from other suspects
5. All collected DNA information is stored in the database

Using DNA from the database
1. Officers collect DNA from a crime scene
2. The police process the DNA from the crime scene and attempts to find a match against the database
3. John's DNA information does not provide a match
4. Jane's DNA information is a match
5. The police pursue further investigation of Jane and is found guilty
6. John is dismissed but his DNA remains on the database
7. Every time the police process DNA John's information will be included even if he is not a suspect.

Potential Extension
The authorities are interested in rolling out a national database that would hold DNA sample from everyone. The police believe that such a comprehensive system will mean that no criminal could possibly escape identification. Additionally, it could serve as a deterrent as the police have information on everyone in the country.

The police are also interested in making use of phones to track the location of people in the country. In conjunction with service providers the police will track and store where people are throughout the day. In doing so, they could link the presence of individuals to the scene of a crime adding weight to DNA identification.

Scenario 6
The government is concerned about terrorism, organised crime, illegal immigration, identity fraud and the provision of government services online. In order to address these concerns, the government wishes to establish a National Identity System.

Solution
The National Identity Scheme is an easy-to-use and extremely secure system of personal identification for adults living in the country. Its cornerstone is the introduction of national ID cards for residents over the age of 16.

Each ID card will be unique and will combine the cardholder's biometric data with their checked and confirmed biographic details. These identity details and the biometrics will be stored on the National Identity Register (NIR). Basic identity information will also be held in a chip on the ID card itself. An Information Commissioner is in charge of ensuring proper use of the NIR.

Use Case Example
Picking up a parcel at the post office
1. Jane goes to the local post office to pickup a delivery
2. The clerk ask Jane for some form of identification
3. Jane hands over her ID card
4. The clerk checks that the card is genuine
5. The clerk compares the photograph to Jane
6. The clerk inserts the card into the card reader
7. Jane enters her pin
8. The pin along with the card information is sent across the network to the NIR
9. The system assigns the transaction a unique number and stores it in the system
10. The NIR system sends back a message confirming that the ID card is valid
11. The clerk hands the ID card back to Jane
12. The clerk hands the parcel over to Jane

Information request by other government agencies
1. A government agency must first have written confirmation from the Information Commissioner to access information from the NIR without consent
2. If the government agency believes that a crime is about to happen
3. The government agency requests for the relevant information from the NIR
4. The NIR sends the government agency the information across a network
6. The agency stores and uses the information as necessary

Possible Extensions What do you think are the likely possible extensions that the government might use the system for?

Appendix III: Individual Study – Survey Questions

As part of the Individual-based study, the following questions were distributed online to UCL university students. Students were instructed to state their level of agreement with the following questions using a 4-point scale (Strongly agree, agree, disagree, strongly disagree).

In order to ground respondents to a similar context, they were provided with scenario 1 from the focus groups (child abuse), and were asked to rate their response in relation to the proposed system.

Situation

exp01	I am aware or familiar with the problem that the government is trying to tackle
exp02	I, or someone close to me, have some experience with the stated problem.
exp03	I have encountered media reports about the stated problem.
ser01	I think that the government is tackling a very serious issue.
ser02	If the government does not tackle these problems, it can lead to unwanted consequences.
ser03	Being affected by the stated problem will negatively affect a person's life.
dep01	Most people have been affected by or are affected by the stated problem.
dep02	The stated problem has an impact on a large part of the population.
dep03	Many people have concerns about the stated problem.
sit01	I think that the stated problem is an issue that needs to be addressed urgently.
sit02	The government must do something to take control of the situation.
sit03	Tools must be developed as soon as possible, that will allow the government to tackle the stated problems.

Information

rel01	I am comfortable with the type of information that the system will collect
rel02	The system is collecting information that is irrelevant to its purpose.
rel03	The system is collecting too much information.
acc01	The system will collect and store a large amount of inaccurate information.
acc02	The system will enable the government to develop an accurate representation of a person in relation to the stated problem.
acc03	The system will hold a lot of wrong information.
use01	The system will allow the government to make better decisions.
use02	The government will be make a lot of mistakes, when using the information stored on the system.
use03	The system will increase the ability of government to tackle the stated problems.
use04	The government will become too reliant on the information collected by the system.

Acceptance

acc01	I would have no objections to the government implementing the proposed system.
acc02	I would willingly enroll and make use of the proposed system.
acc03	I would prefer to the government to use the proposed system, when compared to its current information collection practices.
acc04	I would accept the introduction of the proposed system

Judgment

out01	The proposed system will create an unfair society.
out02	The proposed system will expose individuals to society.
out03	The proposed system will increase the amount of unnecessary citizen tracking.
out04	The proposed system will reduce efficiency when interacting with organizations.
con01	The information stored within the proposed system will leak out.
con02	Insiders working with the proposed system will abuse the information.
con03	The information stored in the system will be held securely.
con04	The personal information collected will eventually be used for some other purpose than the one currently specified.
jud01	I think that the proposed system will be a useful tool for the government.
jud02	I think that the proposed system will be effectice in tackling the stated problem.
jud03	I think that the proposed will take too many resources (cost, time, etc.) to implement and run.

Appendix IV: Individual Study – Survey Analysis

	Component							
	1	2	3	4	5	6	7	8
exp1								.759
exp2								.766
exp3		.458						.533
sev1		.637						
sev2		.714						
sev3		.664						
ext1							.769	
ext2							.767	
ext3		.576						
per1		.757						
per2	.418	.661						
per3	.521	.645						
rel1	.593							
rel2			.447			.437		
rel3			.443					
acu1			.765					
acu2	.405		-.469					
acu3			.733					
use1	.417				.474			
use2			.649					
use3					.613			
use4			.545					
acc1	.679							
acc2	.678							
acc3	.755							
acc4	.721							
out1						.445		
out2						.542		
out3			.460	.416				
out4						.498		
con1				.647				
con2				.498		.553		
con3				-.667				
con4				.776				
jud1					.726			
jud2					.651			
jud3						.463		

All survey question items. Criteria: Eigenvalue >= 1
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.
All survey question items. Criteria: Eigenvalue >= 1
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

	Component										
	1	2	3	4	5	6	7	8	9	10	11
exp1							.794				
exp2							.736				
exp3							.572				
sev1		.718									
sev2		.762									
sev3		.592									
ext1						.785					
ext2						.777					
ext3											.843
per1		.745									
per2		.681									
per3	.499	.670									
rel1	.652										
rel2				.442							
rel3											
acu1				.740							
acu2	.527										
acu3				.824							
use1	.500				.434						
use2				.479						.407	
use3	.482				.564						
use4										.604	
acc1	.737										
acc2	.734										
acc3	.753										
acc4	.750										
out1								.618			
out2								.819			
out4											
con1			.754								
con2			.638								
con3			-.727								
con4			.701								
jud1					.712						
jud2	.496				.603						
jud3									.840		

All survey questions. Criteria: number of factor = 11
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Appendix V: Coding Frames Used for Qualitative Analysis

Individual Study

Code	Coding Rules
Problem Evaluation	Expressions about how important the problem needs to be solved
Exposure (Media)	Mention of information obtained from some media outlet (TV, news, etc.); "I read that…"; Discussion of current events.
Exposure (Personal)	Mention of having work in the field; being affected by the (similar) problem; knowing someone who has been affected by the (similar) problem.
Extent	Talk about the number of people being affected by the problem; the size of the problem ("it's a huge problem"); Comparison about how the system might be more relevant in certain geographical areas because the problem is more frequent there.
Severity	Discussions on the impacts or outcomes of the problem; comparisons to various "levels" of the problem (serious crime vs. non-serious crime); discussions about limiting the use of the system to certain conditions; comparisons about importance of the particular problem to other problems.
System Assessment	Expressions that describe the usefulness or effectiveness of the system in addressing the problem that the identity system is supposed to address.
Info. Relevance (Granularity)	Issues around the amount of information being collected; suggestions to reduce amount of information collected; recommendations to limit information collecting to a higher level (e.g. general broad categories as opposed to specific items).
Info. Relevance (Sensitivity)	Suggestions to tightly control the flow of information; discussions about having the right to the information (e.g. teachers having access to medical records); access controls.
Info. Accuracy (Completeness)	Discussions around the inability of the system to collect all the intended information; gaps in data set specified by the government; not collecting all the information required; gaps in the data collection strategy; constantly changing information.
Information Accuracy (Visibility)	Thoughts on how accessible the information is to the system; difficulty in reading, perceiving, or assigning value to the information collected; difficulty in correctly parsing the information; attributing information to the wrong individual.
Information Accuracy (Subjectivity)	Issues about the generation of information by person other than the individual; mentions of the information collected being rumours or notes; variability of information based on attributes of the information producer (employers mood, etc.); discussions about introducing objective measures, or quantification of information.
Information Reliance (Dependence)	Discussions about a decrease in the job performance of the organization using the system; indications that the organization will ignore cases not flagged up on the system; organizations willingness to support information; discussions to limit the use of information as preliminary investigations.
Information Reliance (Challenge)	Thoughts on the ability of the individual to question what the information says about him/her; being able to provide insecticidal evidence; being able to argue decisions; being prematurely judged.
Outcomes (Freedom)	Limitations placed on everyday life; mentions of impacts on personal choice; suggestions to use voluntary schemes rather than being forced into a system; suggestions to use reactive approaches rather than proactive approaches; tracking; big brother.
Outcomes (Fairness)	Issues around discrimination of individuals in society; being judged wrongly; being singled out.
Security Concerns	Breaches in the system; hackers; abuse of information; insiders.

System Study

Code	Coding Rules
Control Points	Discrete events or processes that involve individuals' identity. It should be emphasized that this is any interaction with the identity, not just points where information is read. A control point can therefore be events where the identity is created, accessed, used, or modified in some way; these events or processes can either involve humans, or may be completely automated (e.g. automated DNA matching procedures).
Subject Engagement	Any description of individuals' involvement during events or processes that involve his/her identity (i.e. at control points). Particularly we are interested if individuals are aware of his/her identity is being created, accessed, used, or modified. We are also interested in where individuals' are during these events; does he/she need to be present during these events; does he/she need to begin the process; does he/she need to be present at some point, so that the event can continue or come to an end.
Population Coverage	Any description of the individuals' who are targeted for involvement. There should be some indication of the amount of discrimination happening within that context; i.e. we need to identify all the people that participate within the context of the implementation, then be able to identify what percentage of those people are actually individuals who are enrolled within the system.
Identity Exposure	Any account of the identity 'leaking' out of the IDMS operating context. Is the system falling into the hands of unauthorized individuals? Is it falling into the public domain? Are individuals' being judged, based on their identity, by people who operate in a completely different context?
Expert Analysis	Statements that point out interpretation of identity, or its attributes, require some sort of training or technical expertise. Need to keep an eye out for any occurrences of some form of subjectivity when reading or writing the identity. Note that this is not in relation to the technical mechanisms that may be complicated, but the actual use or creation of the information.
Population Comprehension	Details about how the general populations mental model of the IDMS. In contrast to *expert analysis*, this covers not only the interpretation of the identity and its information, but also the technical mechanisms behind it; e.g. do they understand how an identity matching procedure takes place? Do they know what is happening in the background? Need to capture how well laymen understand how the IDMS as a whole works, and what the identity or an identity match means. Do they thoughts of the identity and IDMS match reality?
Information Accuracy	Descriptions of the accuracy of the identity attributes collected, and stored within the system. Is the information being attached to an identity correct?
Information Stability	Descriptions of how often the identity attributes changes over time. The frequency with which the relevant information changes. This is distinct from accuracy, as the information may be accurate, but out of date.
Subject Coupling	Any indications that the identity created or used does not fully capture the individual within that context. Look out for situations where individuals' are being prematurely judged based on a particular bit or set of information, instead of taking a complete account of the individual. Also need to keep an eye out for situations where individuals are being judged by information that is not relevant to the context in which he/she is being judged.
Information Variability	Warnings/statements of concern, especially from experts, regarding the use of identity or its attributes for purposes other than the one stated.

Organisation Study

Code	Coding Rules
Purpose	Mention of what the IDMS is supposed to be used for. What problem is it suppose to support? What organisation processes is the identity supposed to inform?
Relying Parties	Any mention of the parties that will access the identity to carry out a task.
Objective (Enablement)	Statements about what the identity information will be used for. Is the focus of the identity on making it easier for individuals' to perform tasks? Or is the focus on making it more difficult to abuse resources? i.e. is the identity being used as a tool to gain access to new services or encourage uptake of existing services, or is it used to add another layer of security to existing resources?
Objective (Proof)	Statements about how the identity will be related across different contexts or organisations. Is the identity being used in such a way so as to be able to easily create an 'identity net' over the individual? Or is the identity only being used as an authentication mechanism, implying there is no way to connect the current use of identity at a later stage.
Accessibility (Information Set)	Mentions over what identity attributes each relying party requires to carry out its task.
Accessibility (Locality)	Specifications over how relying parties will gain access to the identity and its attributes. Will it take place remotely over a network or some backend process? Or can the relying party only gain access to the identity when the individual presents it, i.e. only local access is provided?
Accessibility (Readability)	
Accessibility (Direction)	Specifications over what *relying parties* can do with the identity. Is it only a one-way read access? Or can the *relying party* write or modify the identity or system in some way.
Conditions (Risk Level)	Indications over the danger levels under which the *relying party* may operate. Is the *relying party* dealing with high security issues, and is the identity critical to its task, thus implying a high risk level? Or is the *relying party* non-critical in nature, implying more relaxed requirements.
Conditions (Timeliness)	Indications over the time sensitive nature of *relying parties*. What are the consequences of not getting access to the identity immediately? Could it be potentially disastrous, in which case access should be given immediately, or is a slight delay non disastrous.
Authenticity	Mention of the organisation attempting to enroll the true identities of individuals. Look out for points on collecting documentation or confirming biographical information against some third party.
Uniqueness	Mention of the organisation working to ensure that each individual only has one identity in the system. Pay attention for instances of biometric use.
Obligations (International)	Any mention, debates, or consideration, about requiring to confirm to international standards.
Obligations (Current Practices)	Any mention, debates, or consideration, about previous identifying practices or current practices (by the organisation or related organisations) that influence the organisations choices.
Performance (Accuracy)	Any mention of accurately producing matches of the individual against the identity. Any mention of not being able to do so as well.
Performance (Human Readability)	Any mention of the requirement to have human intervention when interpreting or matching biometrics to an individual.
Population (Size)	Any concerns raised about the number of people that are enrolled or need to be enrolled onto the system. Especially look out for concerns on how that may affect accuracy.
Population (Compatibility)	Any concerns raised about how well the biometric performs against the target population. Are there any characteristics or patterns within the population that negatively affects the accuracy.
Population (Geographic diversity)	Any concerns raised about the geographical landscape that the IDMS has to operate in. Pay attention for remoteness of locations the IDMS has to operate in. Look out for the unavailability of technical equipment.

Appendix VI: Hofstede's Value Survey Module

See Overleaf. Taken from http://www.geerthofstede.nl/vsm-08

V S M 08

VALUES SURVEY MODULE 2008
QUESTIONNAIRE
English language version

Release 08-01, January 2008

hofstede@bart.nl； www.geerthofstede.nl

INTERNATIONAL QUESTIONNAIRE (VSM 08)- page 1

Please think of an ideal job, disregarding your present job, if you have one. In choosing an ideal job, how important would it be to you to ... (please circle one answer in each line across):

1 = of utmost importance
2 = very important
3 = of moderate importance
4 = of little importance
5 = of very little or no importance

01. have sufficient time for your personal or home life	1	2	3	4	5
02. have a boss (direct superior) you can respect	1	2	3	4	5
03. get recognition for good performance	1	2	3	4	5
04. have security of employment	1	2	3	4	5
05. have pleasant people to work with	1	2	3	4	5
06. do work that is interesting	1	2	3	4	5
07. be consulted by your boss in decisions involving your work	1	2	3	4	5
08. live in a desirable area	1	2	3	4	5
09. have a job respected by your family and friends	1	2	3	4	5
10. have chances for promotion	1	2	3	4	5

In your private life, how important is each of the following to you: (please circle one answer in each line across):

11. keeping time free for fun	1	2	3	4	5
12. moderation: having few desires	1	2	3	4	5
13. being generous to other people	1	2	3	4	5
14. modesty: looking small, not big	1	2	3	4	5

INTERNATIONAL QUESTIONNAIRE (VSM 08) – page 2

15. If there is something expensive you really want to buy but you do not have enough money, what do you do?
    1. always save before buying
    2. usually save first
    3. sometimes save, sometimes borrow to buy
    4. usually borrow and pay off later
    5. always buy now, pay off later

16. How often do you feel nervous or tense?
    1. always
    2. usually
    3. sometimes
    4. seldom
    5. never

17. Are you a happy person ?
    1. always
    2. usually
    3. sometimes
    4. seldom
    5. never

18. Are you the same person at work (or at school if you're a student) and at home?
    1. quite the same
    2. mostly the same
    3. don't know
    4. mostly different
    5. quite different

19. Do other people or circumstances ever prevent you from doing what you really want to?
    1. yes, always
    2. yes, usually
    3. sometimes
    4. no, seldom
    5. no, never

20 . All in all, how would you describe your state of health these days?
    1. very good
    2. good
    3. fair
    4. poor
    5. very poor

21. How important is religion in your life ?
    1. of utmost importance
    2. very important
    3. of moderate importance
    4. of little importance
    5. of no importance

22. How proud are you to be a citizen of your country?
    1. not proud at all
    2. not very proud
    3. somewhat proud
    4. fairly proud
    5. very proud

23. How often, in your experience, are subordinates afraid to contradict their boss (or students their teacher?)

1. never
2. seldom
3. sometimes
4. usually
5. always

To what extent do you agree or disagree with each of the following statements? (please circle one answer in each line across):

1 = strongly agree
2 = agree
3 = undecided
4 = disagree
5 = strongly disagree

24. One can be a good manager without having a precise answer to every question that a subordinate may raise about his or her work	1	2	3	4	5
25. Persistent efforts are the surest way to results	1	2	3	4	5
26. An organization structure in which certain subordinates have two bosses should be avoided at all cost	1	2	3	4	5
27. A company's or organization's rules should not be broken - not even when the employee thinks breaking the rule would be in the organization's best interest	1	2	3	4	5
28. We should honour our heroes from the past	1	2	3	4	5

INTERNATIONAL QUESTIONNAIRE (VSM 08)- page 4

Some information about yourself (for statistical purposes):

29. Are you:
    1. male
    2. female

30. How old are you?
    1. Under 20
    2. 20-24
    3. 25-29
    4. 30-34
    5. 35-39
    6. 40-49
    7. 50-59
    8. 60 or over

31. How many years of formal school education (or their equivalent) did you complete (starting with primary school)?
    1. 10 years or less
    2. 11 years
    3. 12 years
    4. 13 years
    5. 14 years
    6. 15 years
    7. 16 years
    8. 17 years
    9. 18 years or over

32. If you have or have had a paid job, what kind of job is it / was it?
    1. No paid job (includes full-time students)
    2. Unskilled or semi-skilled manual worker
    3. Generally trained office worker or secretary
    4. Vocationally trained craftsperson, technician, IT-specialist, nurse, artist or equivalent
    5. Academically trained professional or equivalent (but not a manager of people)
    6. Manager of one or more subordinates (non-managers)
    7. Manager of one or more managers

33. What is your nationality?

    _____

34. What was your nationality at birth (if different)?

    _____

Thank you very much for your cooperation!

Appendix VII: Document provided for Expert Evaluation

See Overleaf

A Human-Centred approach to Identity Management Systems

The research presented here breaks away from the traditional functionalist view of identity, and presents a framework for a human-centred approach to identity management systems (IDMS). Research is based on a qualitative exploration of:

1. the identity system
2. the individuals that are enrolled, and
3. the organisations that implement them.

The aim of this document is to allow experts to evaluate the validity of the framework (see *Figure 2*). When reviewing the framework, experts are asked to consider and provide answers for the following questions:

1. Do the constructs asserted in the organisation sub-framework reflect real-world issues that organisations deal with when implementing of an IDMS (*Section 1.3 2*)?
2. Can the design of an IDMS be decomposed and expressed in terms of the constructs as asserted by the system sub-framework (*Section 1.1)*?
3. Can the constructs of the system sub-framework by used to narrate the lived experience? (*Section 1.1)*?
4. Do the constructs in the individual sub-framework capture individuals' concerns over, and willingness to accept a new IDMS (*Section 1.2)*?
5. Do the hypothesised relationships between the various sub-frameworks within the unified framework have merit (*Section 1.4)*?
6. Are there any other important constructs or relationships that are missing from the unified framework and its sub-frameworks (*Section 1.4)*?
7. Can the framework by used to aid system implementers to design human-centred IDMS?
8. Does the framework help researchers identify potential new areas of research?
9. Does the framework add any value to the identity field?
10. What improvements can be made to the framework?

Glossary - The Identity Ecosystem

This section provides a brief overview of the terms used throughout this document.

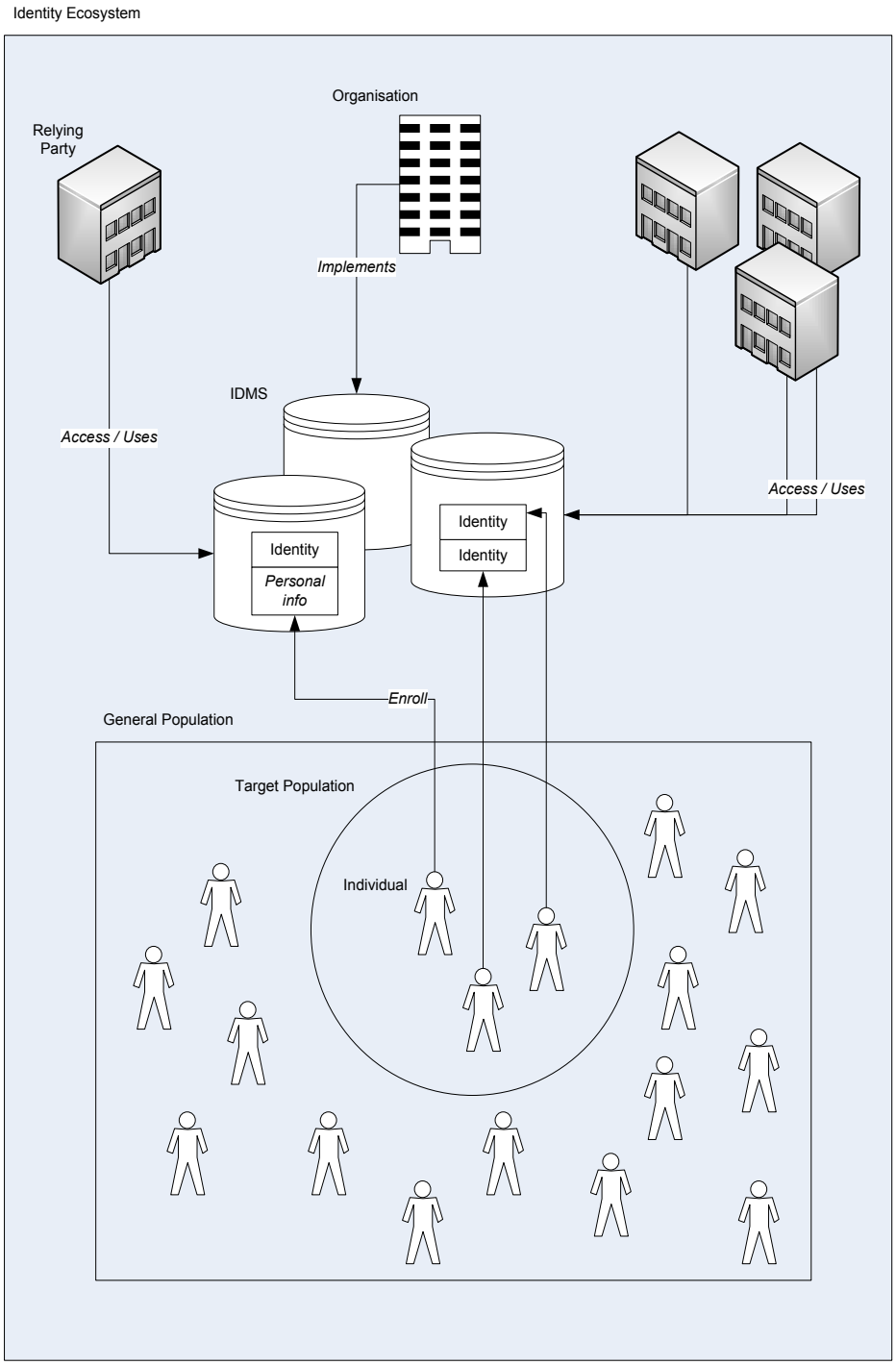


Figure 1 Identity Ecosystem

Table 1 Glossary of terms in the Identity Ecosystem

Term	Definition
Identity	A set of information and attributes about an individual that is collected and stored within a particular context; linked to an identifier(s) that sufficiently identifies the individual within as set of individuals.
Identity Management System (IDMS)	A mechanism that allows for the creation, administration, access, and use of identity.
General Population	All the people that act within the context of the IDMS; this includes people who operate in the context, but may not be enrolled within the IDMS.
Target Population	The section of the general population is required to enrol with the IDMS, so as to continue to operate within the context.
Individual	A single person from the target population that has enrolled with the IDMS.
Organisation	The entity that is in charge of the planning, developing, running, and maintaining a particular IDMS.
Relying Party	An entity that requires access to the IDMS.

1 The Identity Framework

This research represents a first attempt towards building a human-centred IDMS. Traditional approaches to IDMS tend to be functionalist; the far-reaching impacts of the identity on individuals are ignored, reducing *human-centred* discussions to technological issues surrounding data collection, and administrative benefits for organisations. This is in part driven by the traditional organisational view of identity as a mechanism to access resources, and ignores that identity itself has become the strategic resource that is accessed. Hence, the individual is reduced to a functional component, thus eliminating debates around the perceptions and consequences of identity.

Our research approaches the issue of human-centred identity through a holistic understanding of the identity ecosystem (see Figure 1). The result of this research is a unified identity framework that provides a narrative of the entire ecosystem, thus providing practioners with a new tool to guide the development of human-centred IDMSs, while also identifying further areas of research.

The research consisted of three main studies, each of which focused on a major construct within the identity ecosystem:

1. **System-Based Study**
2. **Individual-Based Study**
3. **Organisational-Based Study**

Below is a very brief overview of the findings from each study. This is further explained and clarified in the next chapter, where the findings are applied within the context of a hypothetical IDMS implementation.

1.1 System-Based Study

This study focused on the practical design of an IDMS, and how it can affect the lives of individuals. Results from this study asserts that IDMSs can be broken down into set of **structural and metrical design properties**, which taken together can be used to develop a narrative for the lived experience; i.e. how the design of an IDMS can affect individuals' everyday lives (*see Appendix II for details of the study*).

The **structural properties** describe the flow of an individual's information within the identity ecosystem. It is captured by the following properties:

Structural Property	Definition
Control Points	The number of points where identity is accessed.
Subject Engagement	The degree to which an individual is active at each control point.
Population Coverage	The percentage of the general population that is enrolled; a ratio between the target population and the general population.
Identity Exposure	The degree of control that an individual has in the presentation of his/her identity to the rest of society at each control point.

The **metrical properties** are concerned with the type of information that is captured, and the way it is interpreted or used. It is captured by the following properties.

Metrical Properties	Definition
Subject Coupling	The degree of representativeness between the information collected, and the relevant partial identity.
Population Comprehension	The degree to which general population understands the entire identity process and the technologies used to support it.
Expert Analysis	The level of user involvement or expertise that is required to interpret identity.
Information Accuracy	The level of accuracy of the identity information.
Information Stability	The level of frequency with which the identity information changes.
Information Variability	The degree to which the identity information may be used for purposes beyond those for which it is collected, irrespective of preventative laws that may be enacted to prevent it.

1.2 Individual-Based Study

This study focused on individuals' perception of IDMS, and how that affects the acceptance of such systems. Findings from this study found that individuals' decision to accept an IDMS is driven by their:

1. **Situation perception –** an individual's perception on the importance of finding a solution to the problem that the IDMS supports. It depends on:
    a. **Severity –** an individual's perception of how serious it would be for a person to be affected by the problem.
    b. **Extent –** an individual's perception about the number of people that are affected by the problem.

2. **System judgement –** an individual's thoughts on the effectiveness of the proposed IDMS in supporting the organisation to tackle the problem. It depends on:
    a. **Information quality –** an individuals' perception of the accuracy and relevance of the information being collected, stored and used.

3. **Concerns** – an individual's concerns over any negative consequences of implementing the IDMS (eg. security of the information, attacks on freedom).

1.3 Organisational-Based Study

This study investigated the effect of organisations' identity requirements on the design and implementation of IDMSs. The results show that organisational identity requirements are driven by **purpose**. *What is the goal of the system, and what task is it supporting?* It is this purpose that drives the two main processes that the organisation is concerned with; **identity construction** and **identity use**.

When implementing a new IDMS, organisations seek to ensure the integrity of identities in the system. This study has found that organisations fall back on two main identity requirements during the **identity construction** process, both of which influence the information set attached to an identity created in the IDMS:

1. **Authenticity** – to ensure that the identity, and hence the information, about an individual is true. This is done by collecting, verifying, and storing individuals' biographical information. The choice and source of this information is influenced by:
    a. **Universality** – the percentage of the target population that already possesses accepted form of identity documents. The higher the number, the more the organisation can rely on other organisations verifying the identity of new individuals.
    b. **Intimacy** – the percentage of the target population that is already enrolled within in the system. The higher the number, the more organisations can rely on individuals as introducers of new individuals. For example, parents can vouch for their children.

2. **Uniqueness** – to ensure that an individual does not enrol into the system more than once. This is done by collecting and checking individuals' biometric information. The choice of this information is influenced by:
    a. **Obligations –** technology standards that the IDMS must conform to; these can manifest itself in the forms of international standards and current practices.

b. **Performance –** the operational requirements of the biometric in terms of:
    - **Accuracy –** how accurate the biometric is in producing correct matches.
    - **Human readability** – can the biometric be easily read and matched manually?
c. **Population –** the real world population level characteristics that can affect the performance of the biometric; expressed as:
    - **Size –** the size of the population.
    - **Compatibility –** any characteristics, customs, or habits that might reduce the accuracy or usability of the biometric (e.g. burka and face recognition, labour workers and fingerprints).
    - **Geographic diversity** – how widely spread the population across the context of implementation.

Apart from enrolment, organisations also need to define the manner in which identity will be used; this will have implications on the identity access policies that are implemented. There are several factors that need to be considered during the **identity use** process:

1. **Relying Party** – the parties that need access to the identity so as to achieve the goal of the system.
2. **Objective** – a relying party's intention of accessing the identity; expressed as:
    - **Enablement** – the dominant intention of the relying party to either enable the individual to carry out tasks, or to prevent individuals from carrying out certain actions.
    - **Proof** – the intention of the relying party to either use the IDMS as a proof of individuals identity, or as a tracking mechanism.
3. **Conditions** – the circumstances under which a relying party accesses identity; expressed as:
    - **Risk level** – the security sensitive conditions under which the relying party will access the information. For example, situations that affect national security would be seen to have a high risk level.
    - **Timeliness** – the time constraints under which the access will take place, so as to enable the relying party to effectively fulfil its objective.
4. **Access Requirements** – what kind of access the relying party will need to fulfil its objective; expressed as:
    - **Information set -** what personal information does the relying party need to access or modify.
    - **Direction –** captures the push or pull nature of the identity access, which in turn defines the read (including authenticiton procedures) or write rights of the third party.
    - **Locality –** refers to the spatial mode of access to the identity system. This can either happen locally where the authentication only takes place face-to-face, or remotely where an identity is authenticated against an entry on a database.

Finally, while the **identity enrolment and use** processes were modelled separately, they are not mutually exclusive. Each exerts some influence on the other; the **purpose** of the IDMS is the key factor that links the two models.

On the one hand, the **purpose** of the overall system informs the **authenticity and uniqueness requirements**; for example, a **purpose** that is more inclined towards security sensitive operations would have stricter **authenticity and uniqueness requirements**, when compared to non-security applications. On the other hand, **the choice of biographical and biometric information** can also influence further expansion on the **purpose** of the IDMS; different activities require different information sets. For example, a system that only collects facial photographs cannot later support a system that requires a high degree of assurance through the use of fingerprints.

1.4 Unified Framework

Bringing the findings of the three studies together, the research developed a unified framework that provides a detailed narrative of the identity ecosystem. On the one hand, the organisational requirements will affect the system design, and hence the lived experience. This in turn affects individual perceptions of the system. These relationships are illustrated in Figure 2, and are further discussed in the application of the framework to a scenario.

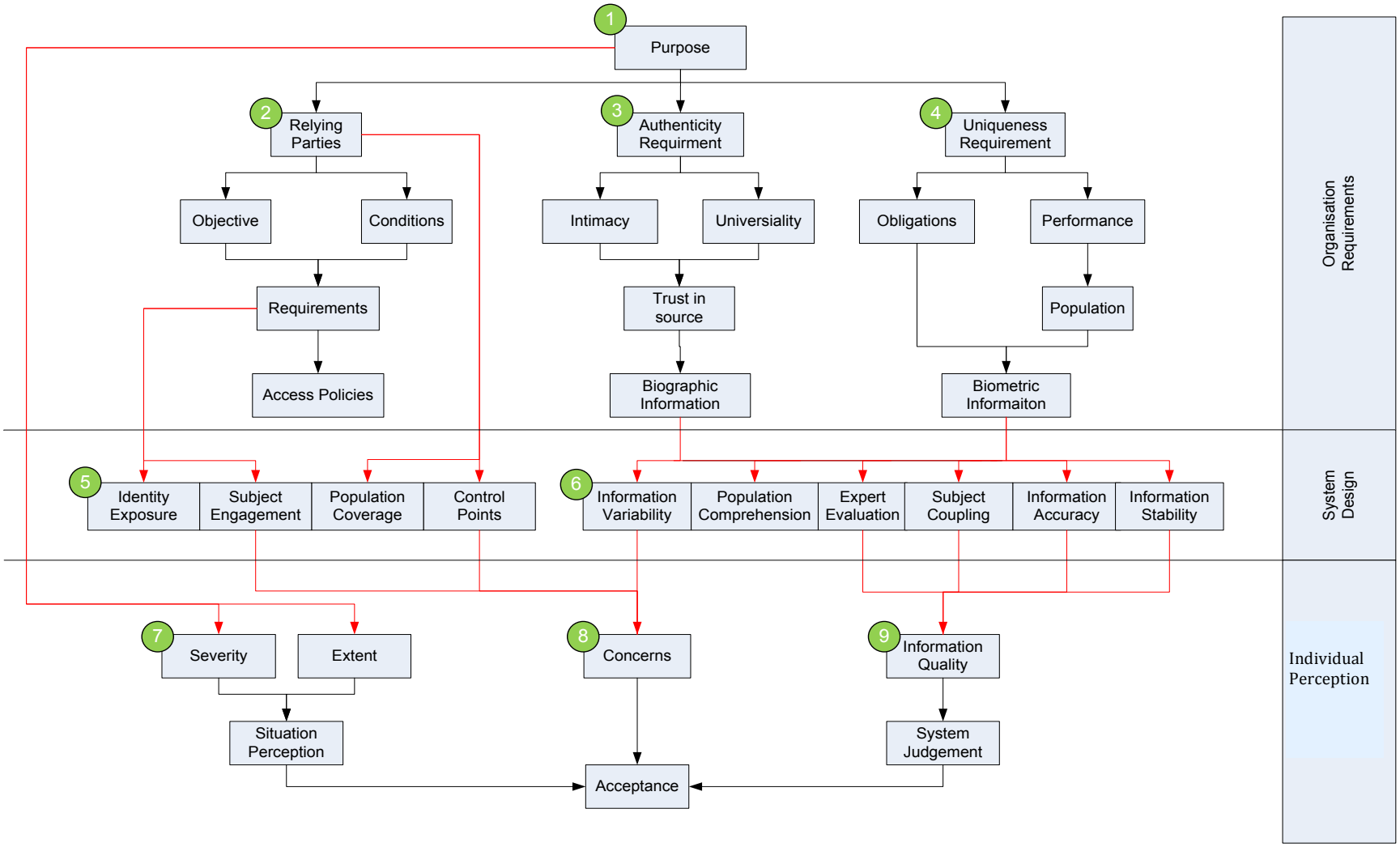


Figure 2 Unified framework (the numbered items in the diagrams serve as place marks that the writing in Section 3 will refer to)

2 Application of the Unified Identity Framework

The unified model can be used as a tool to guide system designers in developing human-centred IDMS that cater for the individual and the lived experience, thus maximising its probability of success. Application of the model takes place in 3 main phases:

1. **Organisational identity requirements are specified**
2. **Design of the IDMS is assessed, along with the offered lived experience**
3. **Initial perception and acceptance is explored**

This section demonstrates a very simple application of the framework within a hypothetical scenario; a UK government organisation seeks to introduce a National Identity Management System (N-IDMS). Using smart identity cards and a centralised database, the aim of the N-IDMS is to:

1. **Provide individuals with a single trusted proof of identity**
2. **Countering Terrorism**

It should be noted that the UK N-IDMS here is loosely based on the recently decommissioned identity system in the country. The system here represents a simplified version that is being used for illustrative purposes only.

2.1 Background in formation on the UK

The United Kingdom has implemented and managed two different identity systems in the past; both were implemented during times of war and uncertainty, World War I and World War II respectively (Agar, 2001), and both systems were ultimately scrapped soon after each war.

The World War I system was used as an aid to conscription. Facing much public opposition, the system fell into disuse once it had fulfilled its purpose. The identity system established in WWII was set to aid in the distribution of rations to the public. However, the system faced much resistance from the public who rejected the *Prussian* qualities of an N-IDMS. This all culminated in the case of John Wilcock who was arrested when he refused to present his identity card to the police upon request; backed by the court and the public, Mr. Wilcocks case was taken to court, where the judge presiding over the case sided with Wilcock. This resulted in the decommissioning of the WWII identity system.

Initial proposals for a new N-IDMS were spurred by the July 2007 bombings, which killed 56 people. This proposal also coincided with government discussions on the creation of a nation-wide citizen identification system; it is believed that such a system would greatly increase efficiency and reduce the costs of both public and private institutions. It is within this context, that the system is being introduced.

2.2 Defining the organisations identity requirements

An IDMS is always implemented for a particular purpose; it is designed to support an organisation in tackling a particular problem. Therefore, defining a purpose is a crucial first step in ensuring that the development of the system is fit for purpose.

1

What is the purpose of the N-IDMS, and how can it help the situation?
Individuals currently lack a single widely acceptance proof of identity. Individuals currently have to use several identity documents to prove identity across various contexts (bank statements, bills, etc). Implementing an N-IDMS will eliminate this hassle, provide a more seamless experience, and provide various relying parties with a single trusted form of identity.

The country is also under threat from terrorist activities. The N-IDMS will help tackle the issue of terrorism by providing the counter-terror unit with access to personal information about individuals that they suspect. Additionally, the use of identity by individuals to access various services can serve as a deterrent for terrorists, and if not, may provide authorities with some useful information that may be recorded (e.g. location, use patterns).

Problem	Aim	Mechanics
Lack of a standard identity document means that individuals are burdened with varying identity proof requirements.	*Reduce hassle of proving identity.*	*Providing everyone with a single widely-accepted and trusted identity document.*
Threats of terrorist attack.	*Counter terrorist threats.*	*Provide the counter-terrorist unit with information about an individual that can aid them in identifying suspects.*

Armed with a specific purpose, the organisation can then begin to define how will be used, after which the required personal information to enable its use will be defined.

2

Which relying parties will need to use or access the identities on the system?
Basic Services and Utilities (Post office, Banks, etc)
Counter-terrorist Unit

What is the objective of the basic services/utilities relying party?
Compared to current identification practices, these relying parties would use the N-IDMS to provide individuals with more seamless access to their services (enablement). Their main intention would be to ensure individuals are who they claim to be (proof).

Enablement:	☒ *Enablement*	☐ *Disablement*
Proof:	☒ *Proof*	☐ *Tracking*

Under what conditions will the basic services/utilities relying party access the N-IDMS?
These relying parties typically don't work under situations that do not pose a direct threat to national security or their operations (low to medium risk level). They may operate under mild time pressures to ensure a seamless service (medium timeliness).

Risk Level:	☒ Low	☒ Medium	☐ High
Timeliness:	☐ Low	☒ Medium	☐ High

What information set do the basic services/utilities relying parties need to access from the IDMS to fulfil its objective?
These relying parties only need individuals' basic personal information to provide their services; therefore the relying parties only need access to:

- *Name*
- *Address*
- *Date of Birth*

What accessibility options will the basic services/utilities relying party require to fulfil its objective?
Depending on the risk level, these relying parties may need varying levels of identity authentication. In low risk situations (picking up a parcel at the post office), a simple visual check of the identity card may suffice (local authentication). However, higher risk situations (opening a bank account) may require a higher level of assurance; a remote authentication against the identity database would be necessary (remote authentication).

As these relying parties only need access to individuals' basic personal information, it has no need to access information on the database. All the required information would be contained on the identity card (local read access).

Based on the counter terrorism purpose, it would be useful to store information (location, time of access, etc.) about any remote authentication onto the database (remote write access).

Authentication:	☒ *Local*	☒ *Remote*	☐ *None*
Read Access:	☒ *Local*	☐ *Remote*	☐ *None*
Write Access	☐ *Local*	☒ *Remote*	☐ *None*

What is the objective of the counter-terrorist unit relying party?

The counter-terrorist unit is focused on finding individuals who are terrorists, and preventing them from carrying out terrorist activities (disablement). Their intention will be in tracking activities of individuals across various contexts (tracking).

☐ *Enablement*	☒ *Disablement*
☐ *Proof*	☒ *Tracking*

Under what conditions will the counter-terrorist unit relying party access the N-IDMS?

The counter-terrorist unit deals with situations that can have severe negative consequences for the whole country (high risk level), and typically work under extreme time pressures to prevent terrorist activities (high timeliness).

Risk Level:	☐ Low	☐ Medium	☒ High
Timeliness:	☐ Low	☐ Medium	☒ High

What information set do counter-terrorist unit relying party need to access from the IDMS to fulfil its objective?

The counter-terrorist unit will need to access all individuals' information stored on the identity system:

- *Name*
- *Address*
- *Date of Birth*
- *Father*
- *Mother*
- *Religion*
- *Fingerprint (forensic use to match fingerprints pulled from scenes)*
- *Facial Portrait*
- *Passport number*
- *Birth certificate number*
- *Audit Trail (location and time of identity use)*

What accessibility options will the counter-terrorist unit relying party require to fulfil its objective?

The counter-terrorist unit does not deal with a party in everyday situations, and therefore has no need for authentication procedures.

Working under high risk and timeliness situations, the counter-terrorist unit will need to have quick access to individuals' identity without their knowledge (remote read access).

The counter-terrorist unit does not provide the N-IDMS with any information about an individual. Additionally, since it operates covertly, any access by the counter-terrorist unit should not be recorded (no write access).

Authentication:	☐ *Local*	☐ *Remote*	☒ *None*
Read Access:	☐ *Local*	☒ *Remote*	☐ *None*
Write Access	☐ *Local*	☐ *Remote*	☒ *None*

Having specified the purpose, and the objectives of all the relying parties, the organisation can then define what information they require to ensure fit for purpose.

3

What <u>biographic information</u> is required to ensure that identities are <u>authentic</u>, and will support the <u>purpose</u> of the N-IDMS?

*As the UK government has had no recent on-going experience with an N-IDMS, the organisation does not know the target population; it has **low levels of intimacy**, and therefore cannot rely on **introducer-based scheme** to ensure authenticity. However, most individuals already possess widely accepted identity documents; the **high levels of universality** imply that the organisation can make use of a **document-based scheme** to ensure authenticity during enrolment.*

As a simple proof of identity, the N-IDMS only requires basic information such as name, address, and date of birth is required. However, as part of an counter-terrorist tool, the N-IDMS may need to hold other information, such as relatives, that could prove to be useful.

Information Item	Source	Universality / Intimacy	Trustworthiness
Name	*Document - Passport*	*Medium*	*Medium*
	Document – Birth certificate	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Date of Birth	*Document - Passport*	*Medium*	*Medium*
	Document – Birth Certificate	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Address	*Document – Electric/Gas/Water bill*	*High*	*Medium*
Father	*Document – Birth certificate*	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Mother	*Document – Birth certificate*	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Religion	*Document - Passport*	*Medium*	*Medium*
Passport Number	*Document - Passport*	*Medium*	*Medium*

4

What biometric information is required to ensure that identities are unique, and will support the purpose of the N-IDMS?

Organisations typically can choose between various different biometrics. In this example, the organisation is considering the use of two of the following three biometrics; fingerprint, iris, or face.

During enrolment the organisation focus on using biometric information is on preserving uniqueness of identities; to ensure that no individuals enrol more than once. This is largely affected by the ***accuracy*** *of the biometric under a one-to-many matching procedure (matching new biometrics to those already stored in the database). The purpose of the N-IDMS also states that it will be used as a proof of identity, implying that the biometric will also be affected by the* ***accuracy*** *a one-to-one authenticator (matching the biometric against a specific entry). This is typically done by specifying the False Rejection and Acceptance rate, which is out of the scope of the current work.*

Performance of the biometrics will also need to hold under real world population considerations. Large ***population sizes****, such as those in the UK, can have a negative effect on* ***performance*** *of certain biometrics (finger print and face). Similarly, certain biometrics may be sensitive to environmental conditions, and therefore would be negatively affected by* ***geographically diverse populations****, such as those in the UK (face).The organisation should also pay attention to the* ***compatibility*** *of the population to the biometric. For example, countries with a large amount of manual labourers would have a negative effect the performance of fingerprint biometric, as the fingerprints of individuals would be worn out from their work (the UK population presents no compatibility issues with any of the biometrics).*

The organisation needs to consider if it needs to fall the biometric to be ***human readable****. This can form a safety net during enrolment; if an individual is falsely flagged as having already registered, staff can then manually match the biometric. Face biometrics adds human readability as staff can just compare photographs; iris and fingerprints do not. So the organisation favours facial recognition technology*

Finally, the organisations choice is also influenced by its ***obligations****. As the biometric is only intended to be used internally, there are no international obligations. However, current practices of related organisations or relying parties may exert some influence. Counter-terrorist units already make use of fingerprints, and so the organisation is inclined to choose fingerprints over iris.*

Information Item	Accuracy	Population Size	Population Geographic Diversity	Population Compatibility	Human Readability
Fingerprint	*Medium*	*Negative effect*	*No effect*	*No effect*	*No*
Facial portrait	*Low*	*Negative effect*	*Negative*	*No effect*	*Yes*

**It should be noted that, for the purposes of simplicity, this document only uses a general measure for accuracy. Any real world application would need to use available accuracy figures.*

2.3 Describing the Lived Experience

Having specified their identity requirements, the organisation can then attempt to describe the implications on the design of the system, and its impacts on the lived experience. It should be noted that, at this stage the rating exercise is a subjective procedure (this is acknowledged in the final chapter).

5

Based on the organisational identity requirements, rate the metrical design properties of the IDMS on a scale of low, medium, or high.

Metrical Properties	Description	Rating
Expert Evaluation	*Biographical information typically lends itself well to being easily interpreted without any specialised knowledge.* *However, the inclusion of biometric systems, especially fingerprints requires expert training. This is especially so in its forensic use by the counter-terror unit.*	*Medium*
Population Comprehension	*Similar to expert evaluation, this is highly influenced by the fingerprint biometric, The general population typically have little understanding of the biometric, and assumes that it is infallible,* *Furthermore, a large section of the general public might not understand how the N-IDMS truly works, especially in the covert use of their information by the counter-terror unit.*	*Low*
Subject Coupling	*Individuals may raise concerns as to why information on parents and religion are collected and stored. It may be perceived as irrelevant especially if they mainly perceive the system as a tool to prove identity to basic services/utilities.* *The use of the system by the counter-terror unit may also raise concerns. Fingerprints carry a large amount of weight within traditional law enforcement circles. Should this trend continue here, and decisions be made solely on the fingerprint, then the relying party would be acting on an incomplete picture of the partial identity.*	*Low*
Information Accuracy	*Relying on trusted sources for authenticity implies that the information collected and stored will be accurate. Additionally, the biometric collected during enrolment will be of high quality as it takes place in control conditions.* *However, the forensic use of the fingerprint by the counter-terror unit serves to reduce the accuracy. Extracting fingerprints from the real world contaminates the information pool, and reduces the overall accuracy of identifications made.*	*Medium*

Metrical Properties	Description	Rating
Information Stability	*The basic personal information set being collected during enrolment remains relatively stable, but may be open to some change. Name and address for example can change over time.* *However, the stability of the identity within the system is reduced when considering the audit trail that is collected over the life time of the identity. New information is constantly being generated, thus creating low levels of stability.*	*Low*
Information Variability	*Fingerprints easily lend themselves to other uses. Specifically, it may be tempting to the police force, who would like to use the identity to track down criminals (as opposed to terrorists).* *Similarly, the identity audit trail can easily be reused for other purposes that again include being used by the police force, to other purposes that sorts the population based on this information.* *Religion is also something to be wary of, as it could possibly be used to discriminate against certain segments of the population at a later date.*	*High*

6

Based on the organisational identity requirements, rate the structural design properties of the IDMS.

Structural Properties	Description	Rating
Control Points	*The N-IDMS has specified a large number of relying parties. Any access to even the most basic of services will require the presentation of identity. This indicates a high number of control points.*	*High*
Subject Engagement	*On the one hand, the organisation has specified that the individual will be present in the access of identity by basic services/utilities. Authentication for example is triggered by the individual, and read access only happens locally. This implies that the individual is active when his/her identity is used, pointing to a high level of subject engagement.* *However, there is also the access of identity by the counter-terrorist unit. Working under high risk and high timeliness conditions, this access of identity needs to take place quickly and covertly. As a result, all access happens remotely, without any authentication procedures triggered by the individual; the individual is in a passive stated, and is unaware of the access and use of his/her identity. This drives down the level of subject engagement.*	*Medium*
Population Coverage	*Like control points, this property is influenced by the number of relying parties specified. Typically, the more relying parties identified, the greater the context in which identity will be used, thus increasing the scope of the target population. In this case, the identity will be used to access all kinds of basic services, implying that the whole population will be covered by the N-IDMS.*	*High*

Structural Properties	Description	Rating
Identity Exposure	*The manner in which the identity is accessed and used will influence the degree of identity exposure. The use by basic services/utilities typically happens on a one-to-one basis in an environment that the individual has a large control over.* *Additionally, the use of the information by the counter-terror unit happens covertly, and will unlikely be broadcast to the public to prevent panic or hysteria. Identity remains un exposed.*	*Low*

Based on the design properties, what kind of lived experience can be expected? How is the individual affected by the collection and used of his/her identity?

Narrating the lived experience requires for the qualitative analysis and exploration of the various design properties, how they influence each other, and its potential negative impacts on individuals' lives, which can derail the success of the system.

Below are several impacts that have been identified:

Lived Experience	Design properties	Description
Burden	*High number of control points* *Medium degree of subject engagement*	*The individual needs to actively produce his/her identity frequently. Failing to do so will lead to the lock out of the individual from accessing even the most basic of services.* *This can create problems of fatigue where the individual feels burdened to constantly carry and present his/her identity document.*
Privacy and freedom concerns	*High number of control points* *Medium degree of subject engagement* *Low level of information stability* *High level of information variability*	*The identity is also accessed frequently without his/her knowledge. This can create feelings of paranoia where the individual feels like he/she is being constantly watched, and therefore cannot act freely.* *The low level of information stability contributes to the feeling of being watched, as the information is constantly changing and being updated. Individuals are being tracked, and thus are further restricted from acting freely* *Furthermore, the other potential uses of the information fuels privacy concerns, and therefore increases the paranoia.*
False accusations	*Low level of subject coupling* *Low level of information*	*Identifying terrorists based only on fingerprints, may result in the possibility of false accusations; a fingerprint does not equate with guilt.*

Lived Experience	Design properties	Description
	accuracy *High level of expert analysis* *Low level of population comprehension*	*The possibility of false accusations happening is increased as the system, used in this forensic context, uses inaccurate fingerprints that are extracted from the real world.* *Furthermore, the expert analysis introduces a level of subjectivity in the identification process, increasing the likelihood of false accusations.* *Finally, as the general population does not understand the identification process, the individual losses the ability the resist such false accusations. He/she does not possess the knowledge to argue his/her innocence, and the general population believes in its infallibility.*

2.4 Determining the general populations' perception of the problem

Once the purpose and design has been defined, the government should then seek out to understand how the general population perceives the situation. In the real world this should be done by distributing surveys developed from the individual-based framework, and using quantitative techniques to identify willingness to accept the system (e.g. likert scales, and statistics).

However, for illustrative purposes, this document will walk though the individual-based framework qualitatively, briefly touching upon the relationship to the system-based framework.

7

What is the individuals' perception of the overall purpose of the IDMS?
*Not being able to prove identity to access services is typically seen to be a **severe** issue as individuals will be locked out from participating in society. However, the **extent** of the population affected by the problem is low; most people have the needed documents to prove identity (bank statements, bills, etc).*

*Similarly, the general population tends to view terrorism as a **severe** problem. However, the lack of recent terrorist activity within the population has dulled individuals' perception of the **extent** of the general population is affected by the problem.*

*Overall, the **high severity positively influences situation perception**, but the **low extent negatively influences the situation perception**, and hence importance placed on introducing a new system to tackle the problems.*

Severity:	☐ *Low*	☐ *Medium*	☒ *High*
Extent:	☒ *Low*	☐ *Medium*	☐ *High*
Situation Perception:	☐ *Low*	☒ *Medium*	☐ *High*

8

Does the design of the system raise any concerns for individuals?
*These concerns may arise in terms of **security concerns** and impacts on **general freedom**. The **high number of control points and the medium level of subject engagement**, offered by the use of a centralised database, fuel these concerns. Individuals will be concerned about the ability of the organisation to **secure the database**, and hence the identities.*

*The covert access of the identity, remotely through the database, **creates paranoia** among individuals of always being watched, and thus creates concerns of freedom. Additionally, the high level of information variability introduces **unpredictability in future use**, raising concerns over individuals' freedom.*

Security:	☐ *Low*	☐ *Medium*	☒ *High*
Freedom:	☐ *Low*	☐ *Medium*	☒ *High*
Concerns:	☐ *Low*	☐ *Medium*	☒ *High*

9

What is the individuals' perception of the information being collected, and how useful do they believe it will be to supporting the purpose of the IDMS?

Individuals' perceptions here are influenced by the metrical design properties of the system. First of all the ***medium degree of information accuracy****, will negatively influence perception of information quality. Similar for* ***the low level of information stability****, as it introduces concerns over the ability of the system to capture all the information that is constantly changing.*

The ***medium level of expert*** *analysis further reduces the overall perception of information quality, as it is seen to introduce subjectivity. Additionally, the* ***low level of subject coupling*** *also serves to* ***decrease perception of information quality****, as the system is seen to collect irrelevant information.*

Overall, perception of ***information quality is low****, implying that individuals system judgement perception would be negative; individuals don't believe that the system would be useful for its purpose.*

Information Quality:	☒ *Low*	☐ *Medium*	☐ *High*
System Judgement:	☒ *Low*	☐ *Medium*	☐ *High*

1

How likely are individuals willing to accept the IDMS?

*Individuals don't see the system as being useful (****low level of system judgement****) to solving a potentially unimportant problem (****medium level of situation perception****). Coupled with the* ***high levels of concerns*** *created, it is unlikely that individuals will accept the system.*

Acceptance:	☒ *Low*	☐ *Medium*	☐ *High*

2.5 Discussion and implication of the unified identity framework on IDMS

Based on the organisations identity requirements, and the resulting design of the N-IDMS, the individual is not willing to accept the system (see Section 3.3; again it should be noted that in a real world implementation, this would be done on a wide scale using surveys). On the one hand, individuals do not believe that the purpose of the system is important. As such, it may be more useful for the organisation to tackle other pressing matters that are perceived to be serious, and impact a large section of the population.

Furthermore, the analysis of the lived experience reveals that the system poses significant threats to privacy and freedom due to tracking, as well as introducing serious risk of innocent individuals being wrongly convicted (see Section 3.2).

Should the organisation choose to proceed with such a system, it should attempt to maximise initial acceptance, and improve the overall lived experience. This would be done by tweaking the various properties of the system design. In this example, the organisation may focus on increasing **information accuracy, information stability, and subject coupling**. This would help to positively influence the perception of **information quality**. Furthermore, the organisation may also seek to reduce the number of **control points**, which posses a low level of **subject engagement**. Doing so can address some of the **concerns** that individuals posses, and hence generate higher rates of **acceptance**.

Tweaking these design properties may create a better lived experience. The higher level of **subject coupling and information accuracy** would reduce the likelihood of false accusations being made. Additionally, the lower number of **passive control points** would reduce the feelings of paranoia and restricted freedom.

Above all these changes would feed back into the organisations requirements. Any changes to the metrical design properties would have an impact on the biographical and biometrical requirements. Changes done to the structural would have implications for the accessibility and objectives of the relying parties. These in turn may require the organisation to reformulate the use and purpose of the IDMS (see Section 3.1)

It should be noted that while the application of the model here is presented in discrete steps, it is likely that these phases will overlap, and occur in tandem. Real life applications may require a rapid prototyping approach where the investigation continuously shifts back and forth between the various frameworks, constantly informing debates, as well as accounting for new concerns, arguments, and possibly changing contextual factors (see Figure 3).

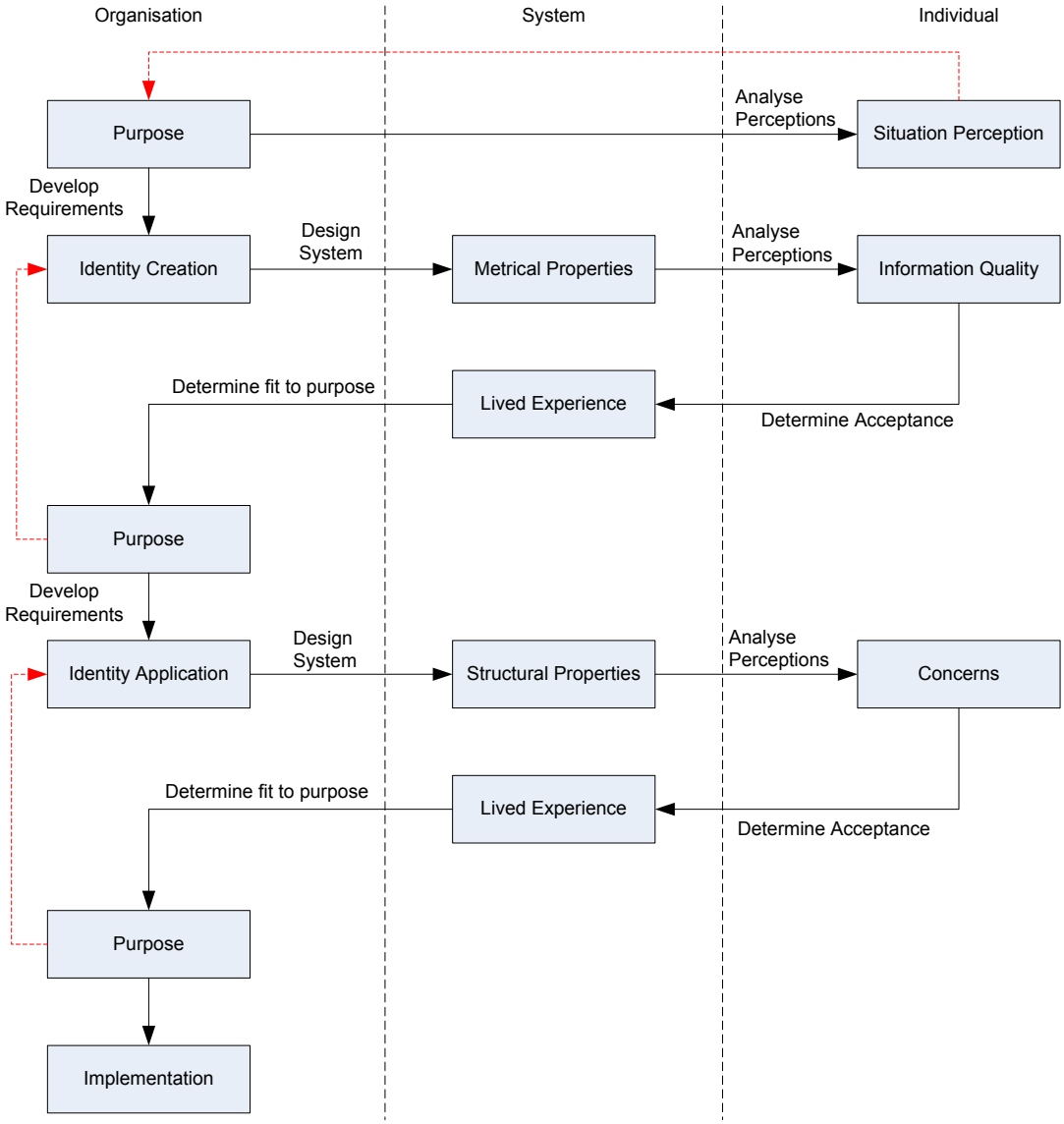


Figure 3 Application of framework in a rapid prototyping approach

Additionally, although it has not been done here, it may be useful to explore the lived experience and individuals' perceptions on a use case basis. In the example here, it may be useful to explore the impacts of the identity use by the basic services/utilities, as separate from the use of the system by the counter-terror unit. This may help to target and reveal specific problem areas that need attention.

3 Future work

With the exception of the individual-based framework, which was supported by a small survey study, the work here has been developed using qualitative techniques. It may be beneficial to take a more quantitative approach, or apply the unified framework to guide a real world implementation; doing so can lend the research greater validity, while providing strong evidence of the relationships between the various sub-frameworks.

It would also be incredibly beneficial to further develop the system framework. At this point, describing the lived experience is a very subjective task. While it encourages the designer to embed the development of the IDMS within its context of use, the lack of proper guidance can hamper efforts. Therefore, it would be useful to develop a mapping between the various properties, and the potential impacts it might have on the lived experience. Similarly, guidance on how to rate the design properties would further reduce barriers to its use.

Furthermore, future work may wish to expand upon the individual framework by including trust constructs that can help to further explain decisions to accept an IDMS. It may also be useful to expand upon the organisation framework, by developing guidelines that help organisations specify the identity requirements.

Appendix I – Alternate scenario based on recommendations

Based on the analysis in Section 3, the organisation has decided to redefine the purpose of the N-IDMS, by eliminating the purpose of counter-terrorism. This requires a re-analysis of the system ensuring that a new design is developed to fit the new purpose.

3.1 Specifying the organisations identity requirements

What is the purpose of the N-IDMS, and how can it help the situation?
Individuals currently lack a single widely acceptance proof of identity. Individuals are currently forced to come to terms with varying identity requirements when proving identity across different contexts (bank statements, bills, etc). Implementing an N-IDMS will eliminate this hassle, providing a more seamless experience, while providing various relying parties with a trusted form of identification.

Problem	Aim	Mechanics
Lack of a standard identity document means that individuals are burdened with varying identity proof requirements.	*Reduce hassle of proving identity.*	*Providing everyone with a single widely-accepted and trusted identity document.*

Which relying parties will need to use or access the identities on the system?
Basic Services and Utilities (Post office, Banks, etc)

What is the objective of the relying party?

Enablement:	☒ *Enablement*	☐ *Disablement*
Proof:	☒ *Proof*	☐ *Tracking*

Under what conditions will the relying party access the N-IDMS?

Risk Level:	☒ Low	☒ Medium	☐ High
Timeliness:	☐ Low	☒ Medium	☐ High

What information set does the relying party need to access from the IDMS to fulfil its objective?

- *Name*
- *Address*
- *Date of Birth*

What accessibility options will the basic services/utilities relying party require to fulfil its objective?

Authentication:	☒ *Local*	☒ *Remote*	☐ *None*
Read Access:	☒ *Local*	☐ *Remote*	☐ *None*
Write Access	☐ *Local*	☐ *Remote*	☒ *None*

3 **What biographic information is required to ensure that identities are authentic, and will support the purpose of the N-IDMS?**

Information Item	Source	Universality / Intimacy	Trustworthiness
Name	*Document - Passport*	*Medium*	*Medium*
	Document – Birth certificate	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Date of Birth	*Document - Passport*	*Medium*	*Medium*
	Document – Birth Certificate	*High*	*Low*
	Introducer – Relative	*Low*	*Low*
Address	*Document – Electric/Gas/Water bill*	*High*	*Medium*

4 **What biometric information is required to ensure that identities are unique, and will support the purpose of the N-IDMS?**

Information Item	Accuracy	Population Size	Population Geographic Diversity	Population Compatibility	Human Readability
Fingerprint	*Medium*	*Negative effect*	*No effect*	*No effect*	*No*
Facial portrait	*Low*	*Negative effect*	*Negative*	*No effect*	*Yes*

3.2 Describing the Lived Experience

5 **Based on the organisational identity requirements, rate the metrical design properties of the IDMS on a scale of low, medium, or high.**

Metrical Properties	Description	Rating
Expert Evaluation	*Biographical information typically lends itself well to being easily interpreted without any specialised knowledge.* *There is not forensic use of fingerprints in this case. Any use of the fingerprints is automated, and therefore no expert that needs to match fingerprints.*	*Low*
Population Comprehension	*The inclusion of fingerprints still presents a small barrier for individuals to understand what is happening..*	*Medium*

Metrical Properties	Description	Rating
Subject Coupling	*Only basic personal information relevant to proving identity is collected and stored.*	*High*
Information Accuracy	*Relying on trusted sources for authenticity implies that the information collected and stored will be accurate. Additionally, the biometric collected during enrolment will be of high quality as it takes place in control conditions.*	*High*
Information Stability	*The basic personal information set being collected during enrolment remains relatively stable, but may be open to some change. Name and address for example can change over time; however this change is not very frequent.*	*High*
Information Variability	*Fingerprints easily lend themselves to other uses. Specifically, it may be tempting to the police force, who would like to use the identity to track down criminals (as opposed to terrorists).*	*High*

6

Based on the organisational identity requirements, rate the structural design properties of the IDMS.

Structural Properties	Description	Rating
Control Points	*The N-IDMS has specified a large number of relying parties. Any access to even the most basic of services will require the presentation of identity. This indicates a high number of control points.*	*High*
Subject Engagement	*The organisation has specified that the individual will be present in the access of identity by basic services/utilities. Authentication for example is triggered by the individual, and read access only happens locally. This implies that the individual is active when his/her identity is used.*	*High*
Population Coverage	*Like control points, this property is influenced by the number of relying parties specified. Typically, the more relying parties identified, the greater the context in which identity will be used, thus increasing the scope of the target population. In this case, the identity will be used to access all kinds of basic services, implying that the whole population will be covered by the N-IDMS.*	*High*
Identity Exposure	*The manner in which the identity is accessed and used will influence the degree of identity exposure. The use by basic services/utilities typically happens on a one-to-one basis in an environment that the individual has a large control over.*	*Low*

Based on the design properties, what kind of lived experience can be expected? How is the individual affected by the collection and used of his/her identity?

Lived Experience	Design properties	Description
Burden	*High number of control points* *High degree of subject engagement*	*The individual needs to actively produce his/her identity frequently. Failing to do so will lead to the lock out of the individual from accessing even the most basic of services.* *This can create problems of fatigue where the individual feels burdened to constantly carry and present his/her identity document.*
Future unpredictability	*High level of information variability*	*Some slight paranoia on the potential use of fingerprints by law enforcement.*

3.3 Determining the general populations' perception of the problem

What is the individuals' perception of the overall purpose of the IDMS?
*Not being able to prove identity to access services is typically seen to be a **severe** issue as individuals will be locked out from participating in society. However, the **extent** of the population affected by the problem is low; most people have the needed documents to prove identity (bank statements, bills, etc).*

Severity:	☐ *Low*	☐ *Medium*	☒ *High*
Extent:	☒ *Low*	☐ *Medium*	☐ *High*
Situation Perception:	☐ *Low*	☒ *Medium*	☐ *High*

8

Does the design of the system raise any concerns for individuals?
The system does not present any significant security concerns, and there are no issues of tracking, reducing concerns over ones freedom.

Security:	☒ *Low*	☐ *Medium*	☐ *High*
Freedom:	☒ *Low*	☐ *Medium*	☐ *High*
Concerns:	☒ *Low*	☐ *Medium*	☐ *High*

9

What is the individuals' perception of the information being collected, and how useful do they believe it will be to supporting the purpose of the IDMS?
Influenced by the high level of information accuracy, and stability, individuals would have a positive view of the information quality. Furthermore, the high level of subject coupling means that the information collected and stored should be seen as being relevant. As a result, system judgement would be positively influenced by the perception of high information quality.

Information Quality:	☐ *Low*	☐ *Medium*	☒ *High*
System Judgement:	☐ *Low*	☐ *Medium*	☒ *High*

1

How likely are individuals willing to accept the IDMS?

Acceptance is likely to be high, as the situation is perceived to be somewhat important, the system judged to be useful, while concerns are kept to a minimum.

Acceptance: ☐*Low* ☐*Medium* ☒*High*

3.4 Discussion and implication of the unified identity framework on IDMS

Based on the new purpose, and the resulting redefinition of the organisation requirements, the new design of the N-IDMS has resulted in a system that individuals are willing to accept. Furthermore, the lived experience has drastically reduced the negative lived experience as previously introduced. Therefore, the system presented here will likely be more successful than the original proposal.

Appendix II – System-Based Study

Using *Thematic Analysis*, a set of 14 past and present N-IDMS were reviewed (see Appendix I), with the aim of tying the outcomes of each IDMS to their specific design aspects. Each system was treated as a unique case study, and a corpus of written work (largely from secondary sources that review the entire situation) centred on each identity scheme was collected for analysis.

Table 2 IDMS reviewed in the system-based study

System	Country	Purpose
Poor Laws and Badges	Untied Kingdom	To provide members of organisations proof of association
Criminal 'Wanted' Lists	-	To provide for accurate identification of individuals especially criminals
Internal Passports	Russia	To track movement of locals in the country
Passports	Netherlands	To prevent or monitor the entry of dangerous foreign radicals into the country
French Nomad Law	France	Identification and monitoring of unwanted members of the population
National ID Cards	United Kingdom Germany	To provide unique identities to individuals allowing easy identification of the entire population.
Bertillonage	France	To identify recidivists enabling enforcement of severe punishment
Dactyloscopy	Argentina	To identify recidivists enabling enforcement of severe punishment
US Visit Programme	United States	To identify criminals and terrorists entering or leaving the country
UAE Iris Scan	United Arab Emirates	To accurately identify known individuals against captured Iris scans (e.g. criminals)
Criminal DNA Database	United Kingdom	To accurately identify individuals against DNA samples
Contact Point	United Kingdom	To identify children in need of protection services before serious harm is caused
PKI and Digital Signatures	Austria	To provide individuals access to services in a virtual environment

Appendix III – Individual-Based Study

A total of 15 *focus groups* were conducted, with an average of 3 participants per focus group. A set of 6 different scenarios were developed to help stimulate discussion within focus groups (Appendix II). Each scenario outlined a hypothetical implementation of an N-IDMS; the scenarios provided details of a problem that a government agency was trying to solve, a proposed identity system, and a use case scenario that described how the system might work. Focus group participants consisted of university students.

Grounded Theory was used to analyse the focus group discussions, which uncovered several different constructs that had an impacted on an ***individual's decision to accept an IDMS***. These were used to develop a hypothesised framework, which was then validated using a small survey study (*excluding the cultural constructs*). A survey was developed and distributed to 668 university students. Keeping in line with the exploratory approach of the thesis, *Exploratory Factor Analysis*, along with *Structural Equation Modelling* was used to develop a good fitting model; this was done by collapsing constructs that loaded highly onto each other, as well as a careful iterative process to eliminating, and introducing theoretically valid relationships into the framework as indicated by the *Structural Equation Modelling* process.

Table 3 Hypothetical scenarios discussed in focus groups

Scenarios	Situation	Solution
Scenario 1	Child Abuse	Any suspicions of child abuse would be noted into a centralised identity system by carer's that came into contact with a child (e.g. doctors and teachers).
Scenario 2	Personal debt	More government control of loaning practices. Centralised government system to collect of personal spending and saving information from stores and across all bank accounts. Information used to calculate risk profile each time a loan is requested.
Scenario 3	Obesity	Use of CCTV and facial recognition to record food purchases at stores and activity levels at gyms. Information routed to central agency, to determine risk of obesity. Advice provided to those who may be at risk.
Scenario 4	Benefit fraud	Employers would enter details of all individuals who are interviewed for a job (commitment, appearance, suitability, etc.), into a centralised system. Information matched to individuals using fingerprints, and used by government agency to assess if individuals are trying to improve their situation.
Scenario 5	Crime	Collection of DNA from all suspects of a crime, including those who are proven innocent. All recorded DNA is used by authorities to match to crime scene evidence.
Scenario 6	Terrorism Illegal immigration	Introduction of identity cards and a national database for the whole population. Cards required to prove identity in various situations from picking up parcel, to accessing government services. Interactions with cards recorded into a centralised database. Law enforcement can access database to investigate security issues.

Appendix IV – Organisation-Based Study

Using a *Case Study* methodology, the study focused on the implementation of N-IDMSs in 3 different countries; Brunei, India and Britain (Appendix III). *Grounded Theory* was used to analyse publicly available documentation on each of the systems; with the exception of the Bruneian case study which relied on interviews, as documentation was not readily available.

Table 4 Cases analysed in the organisation-based study

	Brunei	India	United Kingdom
Date Implemented	2000 – today	2010 – today	2008 – 2010 (abolished)
Purpose	Multi-function smart card	Support poor in accessing services	Prevent terrorism, crime, benefit fraud, travel card
Mandatory	18 and above	All citizens	Voluntary (mandatory for high risk personnel)
Unique ID Number	Yes	Yes	Yes
Identity Card	Yes	No	Yes
Smart Chip	Yes	No	Yes
Centralised Database	Yes	Yes	Yes
Authentication	Against Card	Against Database	Against Card and Database (record authentication on database)
Information Read	Third Parties can access biographical info on card and chip.	Third parties can confirm the accuracy of info (yes/no response only).	Third parties can access biographical info on card and chip. Info can be pushed from the database to third parties. Security organisations may access info on the database
Information Write	Third parties can write to the smart card	None	Info can be pushed from third parties to the database.

Appendix VIII: Feedback from Experts

Professor Andrew Adams

1. Do the constructs asserted in the organisation framework reflect real world issues that organisations deal with when implementing of an IDMS?
It does, but it is incomplete in that it ignores any analysis of likely attackers (those seeking to suborn the system). Such attackers range from terrorists to organised criminals to individuals seeking anonymity to elements of the organisation. Consider the allegations of Israeli government mis-use of foreign passports for a severe example.

2. Can the design of an IDMS be decomposed and expressed in terms of the constructs as asserted by the system sub-framework?
Again, the biggest weakness of this approach is the lack of concept of attacker.

3. Can the constructs of the system sub-framework by used to narrate the lived experience?
There are some missing elements here, such as the ability of the Organisation to impose the system on the target population, which would appear to be a major structural property.

4. Do the constructs in the individual sub-framework capture individuals' concerns over, and willingness to accept a new IDMS?
Some finer grained elements would seem to be needed here. For example, there are a number of types of severity - the severity of a failure of the system for an individual in both false positive and false negative terms. Consider the difference between failed identity checking for payments. Where the individual who is impersonated is liable for the costs then individuals want stronger identity checking. When the whole system is liable then checking is seen as an inconvenience. What is the severity of false negative (payment refused because of identity checking failure for the legitimate subject) compared to the severity of false positive (impersonation)?

5. Do the hypothesised relationships between the various sub- frameworks within the unified framework have merit?
They do, but there are missing dependencies in the graph such as links between population comprehension and identity exposure. Apparent identity exposure and actual identity exposure are different, but related to each other.

6. Are there any other important constructs or relationships that are missing from the unified framework and its sub-frameworks?
Perception/reality differences for some of the elements. The position of attackers and the modeling of cost/benefit models for likely attackers.

7. Can the framework by used to aid system implementers to design human-centred IDMS?
It is certainly a step in the right direction.

8. Does the framework help researchers identify potential new areas of research?
It is a useful contribution to the debate. As presented, there is something of a problem with distinguishing between the views of the researcher and the views of the example subject (the UK IDPA) on the utility of the proposed and now mostly dropped UK ID cards. A better distinction between the framework and the application of the framework to an example case would be needed to help researchers evaluate its contribution.

9. Does the framework add any value to the identity field?
The importance of the lived experience to the design of identity systems cannot be overstated. Any work that highlights these kinds of issues well improves the field.
10. What improvements can be made to the framework?
See earlier comments about attackers and distinguishing between actualities and perceptions, as filtered through comprehensions.

Iain Henderson

In overall terms, I think this framework is a very useful one, and can be built out in many useful directions. It is the first I have seen prepared to operate at such a detailed level; most attempts bail out before the detail (where the devils are...).

I had two specific thoughts on terminology where I felt some improvement could be made; the terms below are where I think greater clarity could be added.

Information' Variability - The degree to which the identity information may be used for purposes beyond those for which it is collected, irrespective of preventative laws the may be enacted to prevent ....

Intimacy – the percentage of the target population that is already enrolled within in the system. The higher the number, the more organisations can rely on individuals as introducers of new.....

Great work, are there any views on how to take this framework into operational reality down the track?

Lothar Fitsch

1. Do the constructs asserted in the organisation sub-framework reflect real-world issues that organisations deal with when implementing of an IDMS?

1.3.2 seems to blend security considerations with business case parameters. Is this intentional? In addition, we feel that compliance management is missing, e.g. privacy compliance. Compliance could be hidden somewhere under "requirements", or under "concerns" at the end of your process diagram. However, for businesses, compliance is a major issue. Cost of ownership of a particular technology, and its potential for future reuse or network effects could be mentioned. I interpreted 1.3.1b ("Intimacy") as "potential for network effects", but I might be wrong here? Generally, some form of corporate risk awareness (how much do we lose on compliance breach, or upon security incidents) could be a valuable addition. Last, not least, a technology-task-fit metric that determines in how far a IDM solution is compatible with the task it should solve would be useful.

2. Can the design of an IDMS be decomposed and expressed in terms of the constructs as asserted by the system sub-framework?

Overall, the system-based properties look usable. Some are vaguely defined, such as "Expert Analysis". It might be worthwhile to look at the "structural property" table, and think of could services and web services. Is your model fit for large-scale distributed could systems with many owners and controllers? I suspect a property of "system fuzziness" indicating the distributedness of the system and its owners/controllers might provide useful additions!

3. Can the constructs of the system sub-framework by used to narrate the lived experience?

What is the sub-system framework? The word doesn't exist in the section 1.1.

4. Do the constructs in the individual sub-framework capture individuals' concerns over, and willingness to accept a new IDMS?

Direct properties such as convenience, and usability, and cost of use seem to be missing from your individual framework. They might fit under "concerns", however.

5. Do the hypothesised relationships between the various sub-frameworks within the unified framework have merit?

Difficult to say. Generally, the 3-division of the diagram makes sense. However, the semantics of the arrows is not clear, as there is no introductory text to the diagram. Is this a flow chart? A sequence? A class diagram? Some of the boxes seem misplaced (however, as they don't get defined extensively, that might just be my subjective judgment).

An important issue is the weighting of factors, e.g. box 8 (Concerns) is a decisive one, which is not clear from the diagram, as it is one of three equal arrows into "Acceptance".

6. Are there any other important constructs or relationships that are missing from the unified framework and its sub-frameworks?

The "business model" of the target system is supposedly hidden in 1) "Purpose"? I can't find a place to put the compliance topic into the diagram. Possibly on the arrow from 1) to 7)?

7. Can the framework by used to aid system implementers to design human- centred IDMS?

The definition of "Human-centered" is not obvious to me. The "human factors" seem solely represented in box 8 "concerns".

8. Does the framework help researchers identify potential new areas of research?

The framework seems to accommodate some of our ideas of privacy risk sources in IDM from the PETweb II project. It might be inspirational for a framework there (see attached article)

9. Does the framework add any value to the identity field?

Hard to say, as the semantics & definitions for all the boxes are not given.

10. What improvements can be made to the framework?

You need better to add definitions of the boxed concepts, and a description of how they relate to specification and prototyping.

Does your work base on some requirements engineering or usability engineering process? There should be a number of references in your text, e.g. about rapid prototyping, requirements engineering, and "human – centered design.

The evaluation case studies that follow the framework are interesting. However, there is little introduction to them, and no explanation how they are related to the framework model. Possibly you could sketch a "process diagram" where you show and explain how the questionnaires and the framework model are used together to make decisions about IDM deployment? The diagram in Fig. 3 is a good start, however its semantics are not quite clear, as e.g. there are two arrows leaving the start box where I was not sure what I should do next.

Following the process, I noticed that the "concerns" box comes rather late – after most things are defined. In my experience, in such a late phase of development, user feedback will, most likely be ignored. Concerns should be evaluated long before the "system design" phase.

Seda Gruses

1. Do the constructs asserted in the organisation sub-framework reflect real world issues that organisations deal with when implementing an IDMS?

Authenticity and uniqueness seem like very important criteria from an organizational perspective for an identity scheme. I am less sure about some of the assumptions that are embedded into those paragraphs:
a) assumptions that parents can vouch for children: this really depends on the context, there are systems where the objective is the opposite: to provide children some protection from their parents. This assumption is negligible and not central to the validity of the rest of your model, however, it does give a normative feeling to the text. This normativity may be the objective of the author, in which case, it should be made more explicit in the beginning of the document.

b) to ensure that an individual does not enroll into the system more than once, you need to collect and check individuals' biometric information: this is a very strong statement. It is true that biometrics do increase uniqueness in an identity system (assuming that the biometric used provides unique results. Uniqueness has been questioned even for DNA databases, but ok, let's hold on to that assumption). However, it is something else to say that they are the pre-condition for uniqueness. For example, my birth certificate has no biometrics on it. There are a reasonable number of identification schemes where organizations do not make use of biometrics. I read the definition of the author for biometrics not to be limited to digital biometrics (i.e., including analog biometrics), but given the context, suggesting that there can be no uniqueness without biometrics throws out all those identification schemes which do not rely on biometrics (in the digital/discretely measured sense of the word). I believe this is a bit too strong of a statement.

Finally, I would expect that the security of biometrics would also play a role for the organization. Let us assume a world where biometrics have been put to use intensively. Let us also assume that there were a number of accidents and these biometric databases were leaked to the public, the biometrics hence become widely available. It is no longer very viable to use these biometrics, as the likelihood of abuse increases. Further, the biometrics themselves have to be secured properly. Otherwise, vulnerabilities of the biometric system could be used to abuse the identity management system (e.g., by replacing the biometric templates of individuals). These are important and costly matters for any organization.

2. Can the design of IDMS be decomposed and expressed in terms of the constructs as asserted by the system sub-framework?

The constructs are rather interesting and helpful. The shortcomings are in their definitions, which are not always very precise. For example:

a) Identity exposure: the degree of control that an individual has in the presentation of her identity to the rest of society... what do you mean by presentation of the identity to the rest of society? do you mean making the identity publicly accessible?

b) Information variability: ...irrespective of preventative laws that may be enacted to prevent it... there seems to be a circular argument here, it is also not clear what is being prevented? :)

A general tightening of the definitions may also increase the readability of the rest of the text. An additional concept to consider is how much control an individual has once the identity has been disclosed? I am talking about the possibility to make use of capabilities similar to "subject access rights" as defined in the data protection legislation, e.g., to ask for transparency, corrections, as well as deletion of data. Further, there are aspects of complaints, things going wrong, and mismatches etc., which are mentioned by the author at different points of the text. It would be nice to have a concept that captures those issues as a separate concern.

3) Can the constructs of the system sub-framework used to narrate the lived experience?

see (2).

4) Do the constructs in the individual sub-framework capture individuals' concerns over, and willingness to accept a new IDMS?

I believe that a number of very important aspects of the lived experience and the resulting willingness to accept are covered by the concepts. However, it seems that the author uses further concepts later on in the paper which are not mentioned in section 1.2: i.e., burden, privacy and freedom concerns, false accusations. It may be better to introduce these concepts in Section 1.2.

There are also further aspects:
profiling and discrimination: I believe this is always appearing in the author's evaluation of the lived experience and easily can be made more explicit. The author may also want to look at Solove's taxonomy of privacy violating activities to see if there are further concerns that you may want to capture. Nissenbaum's concept of contextual integrity may also be relevant to see if further concepts of information flow (what happens to information after identity is disclosed) may be formally integrated into the framework. Currently, the model seems to neglect the life cycle of identity information beyond what is on the tokens, e.g., profiling and tracking over time by linking transactions across contexts using the identity as a basis. The author also mentions paranoia as a concern. This might be the discourse in the U.K., but usually this is referred to as the "chilling effect". You might want to describe the privacy and freedom concerns in those terms without psychologizing individuals, i.e., suggesting they become paranoid. :)

Finally, I believe that what the author is doing is very close to a proportionality test of a planned technology. You may want to look at: Giovanni Iachello and Gregory D. Abowd. Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing. In International Conference for Human-Computer Interaction, pages 91 – 100, 2005. In this article further relevant concepts may be of interest. The article nicely shows that there are matters of acceptability that are beyond the acceptance of systems by

individuals, i.e., is the system acceptable for the society. This is likely to be outside of the scope of framework, but will hopefully be mentioned in the thesis as a necessary element of evaluation of the acceptability of systems.

5) Do the hypothesized relationships between the various sub- frameworks within the unified framework have merit?
I am not sure how to best evaluate the model proposed in Figure 2. I think the text would benefit from a more explicit definition of these relationships. My main problem with the figure is that some entities refer to stakeholders of the system (e.g., relying parties) while others are requirements. I believe that the model would benefit from the introduction of all stakeholders (relying party, organisations (I would prefer to call them identity providers), and individual users) and then you can use those stakeholders' positions to identify the relationships between the elements in the framework. This may of course lead to a more complicated framework, which will have to be balanced with the necessity to keep your framework simple and readable. A challenging work, indeed! I would also imagine that more elements of the framework are related to the concerns of the individuals, currently it reads as if individuals would only have concerns with respect to information variability.

6) Are there any other important constructs or relationships that are missing from the unified framework and its sub-frameworks?
I believe I mentioned them under the different questions above. One thing that is missing in the framework, but it is important to Figure 1: the Identity Ecosystem. Here the figure is assuming a very specific architecture for Identity Management systems. This may be the popular model that is used in the different Identity Management systems the author studied. However, this model has been diversified technologically, and depending on the technical architecture, the roles of the stakeholders as well as the concerns change. I would very much like to see how your evaluation changes not only based on the purpose of the system and user perception, but also based on the type of architecture that is implemented. Specifically, I am thinking of the PRIME/PRIME-LIFE architecture of anonymous credentials, attribute based identity management systems (where it is not necessary to identify the individual but have her prove certain claims etc.) for a short non-technical overview, the author may want to look at the following paper (I apologize for the self-reference): A critical review of 10 years of privacy technology George Danezis and Seda Gürses Surveillance Cultures: A Global Surveillance Society?, April 2010, UK section on privacy as control.

7) Can the framework be used to aid system implementers to design human-centered IDMS?
I am not sure what to think of IDMS and human-centeredness. Unfortunately, most IDMS are constructed to manage populations and are not concerned with user interests. Further, a lot of the problems in the IDMS context occur because the implementers neglect rights that individuals (should) have, e.g., see the case of the U.K. biometric I.D. which has not been scrapped but is only applied to individuals with less rights (immigrants). Making these systems "acceptable" may lead to a further neglect of those rights. Most of the time, individuals are forced to use identity mechanisms if they want to have access to resources, e.g., food, travel, health etc. I would imagine, human-centricity, a so-far undefined concept, to be something else.

However, I believe your framework manages to point to ways of understanding the lived experience of the individuals who have to participate in such systems. In that sense it is an important contribution, as it puts the users of those systems as important stakeholders. I believe further work in this direction may be helpful in guiding the implementation process of "organization-centric" IDMS.

8) Does the framework help researchers identify potential new areas of research?
Absolutely, I really think that the work is a step forward in thinking about how to bring in the lived experience of users. Future work in this direction would benefit from ways of bringing other stakeholders into the evaluation of these systems and an elaboration of the evaluation process, as discussed in Figure 3.

9) Does the framework add any value to the identity field?
see (7) and (8)

10) What improvements can be made to the framework?
The document would benefit from a longer introduction. It took me a long time to figure out where the journey was going. here are some more specific points:
- Figure 1 needs to be revised. According to the figure, an organisation implements IDMS, suggesting that the Relying Party is not an organisation. There are some buildings on the top right hand side, but I am not sure who they stand for? Not all IDMS systems look like this, so the author should document which IDMS system he has in mind.
- the definitions in Table 1 need revising. Again, they assume a type of IDMS in which there is a unique identity across all contexts. If these definitions are based on the 14 systems that the author studied, then this should be made explicit. Otherwise, the author may benefit from studying glossaries coming out if IDM projects for improving the definitions of some of the concepts (see deliverables from PRIME, PRIME Life, FIDIS, GINI, TAS3 in the EU context).

- there are a number of grammatical and spelling mistakes. Taking care of these would improve the text. - part of what the author is doing is technically known as threat and risk analysis. For example, there are also risks with respect to the relationship between the identity providing organization and the relying parties, e.g., the relying party may abuse the identity system in various ways, the relying party also needs to authenticate, audits and other accountability concerns. The author may want to capture these issues more formally, as they are also of interest to the individuals. - the rating used in the evaluation of IDMS is not very articulate. For example, on page 19, when the author evaluates subject engagement, one issue is found to be "high", the other "low", the outcome is hence "medium". It is not clear to me, what the rating in each case refers to, e.g., high impact, high risk, high probability of occurrence, and how high + low = medium? :)

Appendix IX: Example Checklist for Human-Centered IDMS

1. **What is the purpose of the IDMS, and what problem is it supposed to help tackle?**

2. **Who will require use or access the identities on the system?**

List all relying parties (including individuals, i.e. public).

For Each Relying Party

3. **What is the objective of the Relying Party?**

   3.1. Service: ☐Enablement ☐Disablement
   3.2. Function: ☐Authentication ☐ Link individual between contexts

4. **What set of information does the Relying Party need to access from the IDMS to fulfil its objective?**

List each item of information required.

5. **What accessibility options will the third party require to fulfil its objective?**
   5.1. Authentication: ☐Local ☐Remote
   5.2. Identity Access: ☐Local ☐Remote
   5.3. Write Access ☐Local ☐Remote

6. **Under what conditions will the third party access the identity information?**
   6.1. Risk Level: ☐Low ☐Medium ☐High
   6.2. Timeliness: ☐Low ☐Medium ☐High

7. **Who is the target for cnrollment, and what role/partial identity is relevant to the organisation and IDMS?**

8. **Are there any organisations that can claim the authenticity of an individual?**
   8.1. Universality: ☐Low ☐Medium ☐High
   8.2. Trustworthiness: ☐Low ☐Medium ☐High

9. **Are there known and enrolled individuals on the IDMS who can vouch for un-enrolled individuals?**
   9.1. Intimacy: ☐Low ☐Medium ☐High
   9.2. Trustworthiness: ☐Low ☐Medium ☐High

10. **What information is being collected to ensure the authenticity of the relevant identity?**
List each item of information being collected or attached to identity.

Information Item	Source	Universality / Intimacy	Trustworthiness

11. **How will the uniqueness of the identity be ensured and preserved?**

_____

_____

12. **What are the performance metrics required for authentication?**
    - **12.1. False Rejection Rates:** _____
    - **12.2. False Acceptance Rate:** _____
    - **12.3. Human Readability:** ☐Required ☐Not Required

13. **Under what environmental conditions will the uniqueness information be collected?**

_____

_____

    - **13.1. Spread:** ☐Low ☐Medium ☐High
    - **13.2. Control:** ☐Low ☐Medium ☐High

14. **Are there any requirements to adhere to biometric standards?**
    - **14.1. International:** _____
    - **14.2. Current Practices:** _____

15. **What information is under consideration to preserve uniqueness, along with performance metrics?**

Information Item	False Rejection Rate	False Acceptance Rate	Population Effect	Environmental Effect	Human Readability

16. **Based on all the information in Q1 to Q15, assess and rate system level design properties of the system.**

Structural Properties	Rating	Metrical Properties	Rating
Control Points		*Expert Analysis*	
Subject Engagement		*Population Comprehension*	
Population Coverage		*Subject Coupling*	
Identity Exposure		*Information Accuracy*	
		Information Stability	
		Information Variability	

17. **Based on the design properties, what kind of lived experience can be expected? How is the individual affected by the collection and used of his/her identity?**

_____

_____

18. **What is the individuals' perception of the overall purpose of the IDMS?**
    - **18.1. Extent:** ☐Low ☐Medium ☐High
    - **18.2. Seriousness:** ☐Low ☐Medium ☐High
    - **18.3. Overall Importance:** ☐Low ☐Medium ☐High

19. **What is the individuals' perception of the information being collected, and how useful do they believe it will be to supporting the purpose of the IDMS?**
    - **19.1. Information Quality:** ☐Low ☐Medium ☐High
    - **19.2. System Usefulness:** ☐Low ☐Medium ☐High

20. **What is the individual perception of the overall purpose of the IDMS?**
    - **20.1. Extent:** ☐Low ☐Medium ☐High
    - **20.2. Seriousness:** ☐Low ☐Medium ☐High
    - **20.3. Overall Importance:** ☐Low ☐Medium ☐High

21. **Do individuals' have any concerns about the security of the information and any implications on their overall freedoms?**
    - **21.1. Corruption:** ☐Low ☐Medium ☐High
    - **21.2. Insider Abuse:** ☐Low ☐Medium ☐High
    - **21.3. Hackers/Attacks:** ☐Low ☐Medium ☐High
    - **21.4. Freedom:** ☐Low ☐Medium ☐High

22. **How likely are individuals' willing to accept the IDMS?**
    - **22.1. Acceptance:** ☐Low ☐Medium ☐High

Appendix X: Description of System Based Properties

The following (see overleaf) provides an alternate reading to the System Study (Chapter 5).
It is the article published in the IDIS 2010 journal, and is written differently, which may further aid understanding.

While Chapter 5, describes the findings, it does so in the context of the overall analysis procedure. On the other hand, the following article focuses wholly on the findings of the research, i.e. the article is structured in such a way that each design property is introduced, explained, and exemplified atomically, and thus provides further clarity if needed.

IDIS (2010) 3:605–638
DOI 10.1007/s12394-010-0078-3

A framework for the lived experience of identity

Adrian Rahaman · Martina Angela Sasse

Received: 29 June 2010 / Accepted: 25 October 2010 / Published online: 20 November 2010

Abstract This paper presents a framework for the design of human-centric identity management systems. Whilst many identity systems over the past few years have been labelled as *human-centred,* we argue that the term has been appropriated by technologists to claim moral superiority of their products, and by system owners who confuse administrative convenience with benefits for users. The framework for human-centred identity presented here identifies a set of design properties that can impact the lived experience of the individuals whose identity is being managed. These properties were identified through an analysis of public response to 15 historic national identity systems. They capture the practical design aspects of an identity system, from structural aspects that affect the flow of information - *Control Points, Subject Engagement, Identity Exposure, Population Coverage*—to the metrical aspects that considers how information is used and perceived—*Expert Interpretation, Population Comprehension, Information Accuracy, Information Stability, Subject Coupling, Information Polymorphism*. Any identity system can be described in terms of these fundamental properties, which affect individuals' lived experience, and therefore help to determine the acceptance or rejection of such systems. We first apply each individual property within the context of two national identity systems—the UK DNA Database and the Austrian Citizen Card, and then also demonstrate the applicability of the framework within the contexts of two non-government identity platforms—Facebook and Phorm. Practitioners and researchers would make use of this framework by analysing an identity system in terms of the various properties, and the interactions between these properties within the context of use, thus allowing for the development of the potential impacts that the system has on the lived experience.

Keywords Identity · Identity management system · Privacy · Trust · Design · Lived experience

A. Rahaman (✉) · M. A. Sasse
Computer Science, University College London, London, UK
e-mail: a.sallehabrahaman@cs.ucl.ac.uk

M. A. Sasse
e-mail: a.sasse@cs.ucl.ac.uk

Introduction: identity systems today

Identity is a construct that underlies the mechanisms which enable or prevent an individual from performing certain actions in a social environment. Many organisations seek to obtain—explicitly or implicitly—reliable proof of individuals' identities, to ensure effective policing of their rules and policies. Ashbourn (2000) describes how administrators in ancient Egypt used anthropometric techniques to identify workers claiming their food rations, to prevent them collecting rations more than once. Anthropometric techniques were used in France as a means of identifying recidivists, so authorities could give them harsher sentences than first-time offenders (Caplan and Torpey 2001). With the increasing use of IT systems, there is a growing disembodiment of identity processes; interactions that were previously conducted face-to-face, and using physical documents as evidence, are now mediated through information and communication technology (Giddens 1991; Lyon 2002). There has been a flurry of research in how to best represent and manage identities in this context, and a number of different schemes and technologies have been proposed, designed and implemented.

In the private sector, the eagerness to identify individuals and collect information about them is driven by the promise of new revenue streams through the provision of 'customer-centric' personalized services. Recommender and social networking systems rely on the aggregation of various types of information about individuals—the resulting identity profiles allow third parties to judge the trustworthiness and the authenticity of each respective individual (O'Donovan and Smyth 2005). The public sector wants to harness similar approaches to reduce the costs of service delivery and increase convenience through 'citizen-centric' services and data-sharing (Silcock 2001).

There is however, a risk that the labels 'customer-centric' or 'citizen-centric' remain a statement of intent, because the *needs and wishes* of individual customers and citizens, and the impact of identity systems on their *lived experience,* are rarely considered during the design process. The concept of *lived experience* increases the scope of human-centred design beyond traditional usability concepts, which are *"directed more toward functional accounts of computers and human activities"* (McCarthy and Wright 2004). Designing for the lived experience requires an understanding of "*the relationship between people and technology in terms of felt life and the felt or emotional quality of action and interaction*" (McCarthy and Wright 2004). Current approaches to human-centered identity do not consider the impact on lived experience. For example, in a report sponsored by the Information Commissioner's Office (Workgroup on User-Centric Identity Management 2008), discussions on empowering individuals were focused on the 3 traditional pillars for human-centred design:

1) Usability—Making identity systems simple and easy to use reduces barriers to adoption.
2) Privacy—Privacy concerns are a major factor in the adoption of identity systems. These systems can involve the transfer of sensitive information between different parties. Protecting privacy is important so as to prevent personal information from falling into the wrong hands which can erode autonomy and freedom.

3) Trust—The degree of trust that individuals have in the organisation collecting identity information mediates their concerns about privacy. High trust will increase adoption of an identity system (Adams and Sasse 2001).

The discussions of the three aspects of identity systems are utilitarian—essentially seeking to enable organisations to obtain individuals' consent for collection and sharing of information. It does not consider the more far-reaching impact of the use of identity information on individuals, reducing the 'human-centred' discussion to the technological issues surrounding data collection, and administrative benefits for organisations. Not considering citizens' needs and perceptions can affect the adoption of such systems. Inglesant and Sasse (2007) conducted a series of case studies on e-government systems commissioned to improve public transport in London, and found that design and implementation decisions led to systems that did not match citizen requirements, and often prompted citizen behaviour that undermined the policy those systems were supposed to support. This affects adoption rates systems, and even in situations where citizens have little choice but adopt them—creates an adversarial stance between the citizens and the owner-organisation, which in turn increases the operational cost of such systems. Given that many e-Government systems are commissioned to reduce cost, systems that create an adversarial stance are counter-productive.

While citizens and customers have accepted some of the new identity systems, they have also voiced their disagreement in other cases. Facebook users protested when profile updates were broadcast (Hoadley et al. 2009), and there have been campaigns against the introduction of national identity systems (Greenleaf and Nolan 1986; The Register 2002; Davies 2005). In other cases, such as the Austrian Citizen Card (Meints and Hansen 2006), there has been a lack of adoption. The problem is that—despite claims that these technologies provide human-centred identity solutions—most systems have been based on what is technically feasible, and convenient from an administrative point of view. The needs and concerns of citizens or customers are often assumed by those commissioning and designing the identity solution, rather than researched (Lips et al. 2005). The impact on the *lived experience* of different citizen groups is rarely considered during design, or monitored after implementation.

In this paper, we present a framework that can be used to assess the design of an identity system from the perspective of *individuals*, accounting for the potential affects of the system on the lived experience. An *individual* here is defined as the person whose identity and information is collected, stored and used within the system. Current approaches to the development and analysis of identity systems lack understanding of how identity systems *practically* affect individuals in their day-to-day interactions within a society, and how this can affect them. The proposed framework expands beyond these traditional boundaries by shifting focus onto the *identity ecosystem* as a whole, recognizing the relationships that exist between the individual, the system and society.

In "Human-centred identity: related models", we present a critical review of existing identity management frameworks and systems that claim to be human-centred. "A new framework: discovering the lived experience of identity" describes how the framework emerged as a result of a thematic analysis of 15 past and present

national identity systems. The core elements of the framework are presented in "Structural properties" and "Metrical properties". "Combining properties" discusses how those properties relate to each other, and how certain combinations within an identity system can impact individuals' lived experience.

"Applying framework to non-government identity systems" applies the properties to non-government systems—Facebook and Phorm. This serves to illustrate the generalizability of these properties and also acts as a form of validation. "Discussion and conclusion" serves as a conclusion and discussion point for the proposed framework. The strengths and weaknesses of the framework are examined, and scope for further work and improvements is provided.

Human-centred identity: related models

There is a growing body of research on identity management that focuses on the human element in identity systems. Much of the research is focussed on making identity systems easier to use (Cameron 2005; Bramhall et al. 2007; Jøsang et al. 2007), issues of privacy (Bramhall et al. 2007; Cavoukian 2009; Camenisch et al. 2005; Berthold and Köhntopp 2001) and trust (Xin 2004; Backhouse and Halperin 2007) but does not consider the impact on an individual's lived experience.

The 7 laws of identity

Developing the concept of the identity metasystem, Kim Cameron (Cameron 2005) put forward 7 rules of identity. An identity metasystem is a unifying framework that enables the integration of different underlying identification technologies, enabling different identity platforms to work through a standardized interface. These rules have become an accepted standard for identity systems. The rules that have been defined are:

1. User Control and Consent
2. Minimal Disclosure for a Constrained Use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Integration
7. Consistent Experience Across Contexts

These 7 rules represent a foundation for eliminating the *"patchwork of identity one-offs that is currently available on the internet"* (Cameron 2005). However, they focus on individuals as *users of the system*, and tackle usability issues that individuals encounter when using identity systems; the aim is to give users control and allow them to make decisions that reflect their preferences. For example, individuals should understand which organisations will receive their information, and agree to the uses that the organisation makes of their personal information.

While Cameron's 2nd and 3rd laws on constrained use and justifiable parties address certain non-interaction issues on the use of information by the consuming party, the aim is to ensure that the individual is aware of how the information is used,

and by whom. It does not consider why an individual might be reluctant to provide certain information to certain parties. While the laws provide a useful set of user-centred design principles, they do not examine the impact of the system beyond the point of interaction.

Privacy

Privacy is a multi-dimensional concept that incorporates the physical, psychological, interactional and information domain (Burgoon 1982; Davies 1997; Decew 1997). Privacy assessments of identity systems typically fall into the informational privacy domain (Smith et al. 1996). This results in a set of best use practices, which are integrated into the development of new Privacy Enhancing Technologies (PETs) (Goldberg 2003), or as guidelines for the development of laws that aim to minimise threats to privacy. Various privacy laws and standards exist: the UK Data Protection Act (DPA), the FTC Fair Information Practices (FIP), or the more recent Global Privacy Standard (GPS). The GPS has been proposed as a "*single harmonized set of universal privacy principles*". The GPS consists of 10 privacy principles (Cavoukian 2010):

1. Consent
2. Accountability
3. Specific Purposes
4. Collection Limitation (Data Minimization)
5. Use, Retention and Disclosure Limitation
6. Accuracy
7. Security
8. Openness
9. Access
10. Compliance

These principles provide a foundation for an individual's rights over the collection and use of his/her personal information by organisations. However, these codes of conduct also seek to promote business through the "*free and uninterrupted (but responsible) flow and uses of personal data"* (Cavoukian 2009). While there is a need to balance individual and organisational needs, these principles are focused on the practices of the organisation, and not on the impact to the individual. For example, the collection of information for a specific purpose does not account for the individual's perception of that purpose. In systems where participation is voluntary, the principle of consent allows individuals to act on their perceptions. However, the privacy principles do not help us to understand why individuals would not consent. While privacy principles can restrict organisational usage of an individual's data, they do not help to generate consent from the individual to provide his/her information. Individuals are considered as customers instead of actors in the identity ecosystem.

Xin's trust model

Xin (2004) developed a comprehensive model of trust that aims to predict individual trust intentions towards National Identity Systems, determining the likely adoption

of the system (Fig. 1). This approach can be seen as being more human centric when compared to the 7 laws of identity and the privacy approaches seen previously. While the trust model lacks grounding in large empirical studies, its development is based on existing recognized models, such as the Theory of Reasoned Action (Fishbein 1975) and Theory of Planned Behaviour (Ajzen 1985).

An individual's trusting intention towards identity system depends on 3 assessments that the individual makes about the context:

1) the individual's positive/negative *Attitude* towards the trusting action
2) his/her judgment on the *Subjective Norms*
3) the individual's *Perceived Behavioural Control*

Each judgement, in turn, is determined by a set of behavioural, normative and control beliefs. Beliefs are the "*subjective probability of a relation between the object of belief and some other object, value, concept or attribute*" (Fishbein and Ajzen 1975). The beliefs influence the judgements:

1) *Behavioural Beliefs* influence *Attitude*
2) *Normative Beliefs* influence *Subjective Norm*
3) *Control Beliefs* influence *Perceived Behavioural Control*

Finally, beliefs are built on specific contextual properties. Building on other trust literature, Xin's (2004) developed a set of context-specific variables for National Identity Systems. These variables called 'bases' consist of the personality, cognitive, calculative and institutional base. Through empirical research, it was established that:

1) *Cognitive Base* determined behavioural and *Normative Beliefs*
2) *Calculative Base* affected the *Normative Beliefs*
3) *Personality Base* influenced the *Institutional Base*

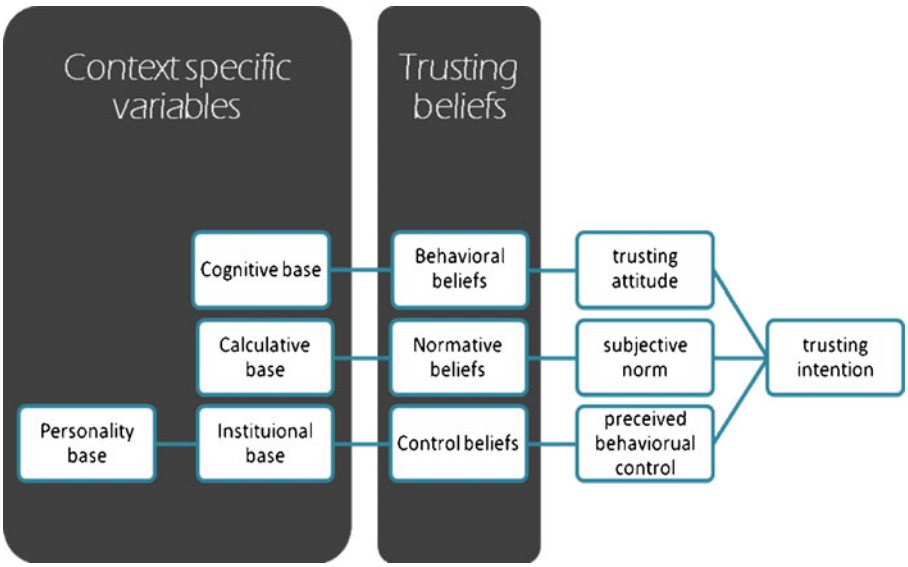


Fig. 1 Xin's trust model towards national IDMS

4) *Institutional Base* influenced an individual's *Perceived Behavioural Control*.

While the model is comprehensive, it does not support designers aiming to build a human-centred identity system since the trusting bases, attitudes and beliefs are only an individual's opinions about performing the trusting action, e.g. signing up for the National Identity System. It does not link the trust model to the actual design of the system. The contextual variables are not connected to any specific implementation details. The framework can help implementers understand an individuals' general thought processes in the development of trusting intentions, thus enabling the creation of more trusting situations. For example, recommendations to increase trust based on this model include the use of focus groups to generate positive feedback that can be publicised to manipulate the perceived reputation of the system (Xin 2004). Effectively, these recommendations are limited to the manipulation of the situational constructs that the system is implemented in, as opposed to detailing how the system itself can influence the *lived experience,* and hence trust.

Table 1 Definitions of construct's in Xin's trust model

Construct	Definition
Attitude	People's evaluation of trusting in NID systems when the government implements them nationwide in the near future.
Subjective Norm	How the people important to you think you should or should not make yourself vulnerable to NID systems when the government implements them nationwide in the near future.
Perceived Behavioural Control	Peoples perceived internal/external opportunities and constraints on being vulnerable to NID systems when the U.S. government implements them nationwide in the near future.
Behavioural Beliefs	Peoples perceptions and information about the consequences of trusting NID systems.
Normative Beliefs	Peoples perceptions and information about the others' opinions on NID systems.
Control Beliefs	Peoples perceptions of their ability, their knowledge about the recourses, opportunities, and constraints of trusting in NID systems.
Personality Base ○ Faith in humanity ○ Trusting stance	Peoples general tendency to trust an object
Cognitive Base ○ Reputation ○ Stereotyping ○ Illusion of Control	Various cognitive cues and impressions on which people form their trusts
Calculative Base ○ Benefits vs. Costs	Refers to some calculative processes involving perceived cost and benefit of performing the trusting behaviour.
Institutional Base ○ Situational Normality ○ Structural Assurance	The impersonal structures that are inherent in a specific circumstance and facilitate trust building in this circumstance

A new framework: discovering the lived experience of identity

Analyzing identity schemes from the traditional usability, privacy and trust perspective abstracts the identity system from the specific consequences that it has on individuals' lives and the various coping strategies that might be adopted. We talk about 'data minimisation' or 'ease of use', but what does it mean to an individual? How does it affect an individual's relationship with the organisation and society? The current frameworks have been useful for the development of better systems, but in applying these principles we lose sight of the entire context of implementation, i.e. the *identity ecosystem* that recognizes the relationships that exist between the individual, system and society. Therefore, the claim that an identity system is human-centred is largely rhetorical; we assume that individuals want better controls and collection of less data, but we have no idea as to how and under what conditions it affects their perceptions. For example, the advertising platform Phorm was deployed by Internet Service Providers with the intention to serve personalised advertisements, based on an individual's online browsing habits. Although privacy experts had given the system their approval, Phorm still raised privacy concerns for customers leading to protests and vigorous opposition (BBC, 2008b).

Practitioners and researchers require a way of analysing the lived experience that results from participating in an identity ecosystem. We require a framework that will allow them to assess how the designs of an identity system might influence an individual's perception of the context, and therefore how the system can shape an individual's reactions when encountering such systems.

Methodology

A tool aiming to assess the impact of an identity system design should be expressed as a set of configuration properties into which any such system can be decomposed. We have identified these properties through a review of past and present National Identity Systems. The scope of that review was limited to National Identity Systems in the Western world, largely focusing on a timeframe extending from the medieval periods to the present day, as these countries have been leading the development and adoption of modern identity systems (Torpey 2000).

The systems that formed the focus of the review (see Table 2) were implementations of Identity Systems that supported the development of Nation States, its control over migration and crime, and the provision of welfare and services. The aim of the analysis was to tie the known outcomes of each system to specific design aspects. Each system was treated as a unique case study, and a *corpus* of written work (largely from secondary sources that review the entire situation) centred on each identity scheme was collected for analysis.

Thematic Coding (Marks and Yardley 2004; Flick 2002) was used to identify similarities across the narratives of the various past and present national-scale identity schemes. Thematic coding is a qualitative research method the makes use of a constant comparison paradigm between several case studies, attempting to identify patterns that relate to the phenomena of interest. The method enables the identification of themes across different contexts from large volumes of data. Our analysis treated each national identity system as a separate case, and identified

Table 2 National identity systems analyzed

System	Country	Purpose
Poor Laws and Badges	United Kingdom	To provide members of organisations proof of association
Criminal 'Wanted' Lists	–	To provide for accurate identification of individuals especially criminals
Internal Passports	Russia	To track movement of locals in the country
Passports	Netherlands	To prevent or monitor the entry of dangerous foreign radicals into the country
French Nomad Law	France	Identification and monitoring of unwanted members of the population
National ID Cards	United Kingdom Germany	To provide unique identities to individuals allowing easy identification of the entire population.
Bertillonage	France	To identify recidivists enabling enforcement of severe punishment
Dactyloscopy	Argentina	To identify recidivists enabling enforcement of severe punishment
US Visit Programme	United States	To identify criminals and terrorists entering or leaving the country
UAE Iris Scan	United Arab Emirates	To accurately identify known individuals against captured Iris scans (e.g. criminals)
Criminal DNA Database	United Kingdom	To accurately identify individuals against DNA samples
Contact Point	United Kingdom	To identify children in need of protection services before serious harm is caused
PKI and Digital Signatures	Austria	To provide individuals access to services in a virtual environment

features of each system that led to the documented responses from the various stakeholders. The analysis took place in three main phases:

1. Reviewing an authoritative and recognized documentation of each implementation, determining the degree of adoption, and the various reactions towards the system implementation. Did individuals sign up to a voluntary system? Did they attempt to evade non-voluntary systems? Did they change their habits as a result of being part of the system?
2. Discover the arguments that lead individuals to react in the manner identified- how did they feel about the system?
3. Code the basic features, i.e. the design properties of the system that brought about the identified reactions of individuals.

As a brief example, the analysis of the use of badges under the Poor Laws in 17th century England began by identifying the theme of rejection among the individuals who were to enroll into the system (Caplan and Torpey 2001; Carroll 1996). Analysing the main documentation, and where required accompanied by relevant support material, we found that rejection stemmed from feelings of shame that arose from being registered in the scheme. We can then identify the characteristics of the system that

triggered these emotions the feelings of shame were triggered by the constant wearing of the badges, which exposed a small set of individuals to the rest of the population.

These system characteristics formed the basis of the coding procedure in the analysis. The codes were developed to express basic design aspects of an identity system. Using the above example, we code 'the need to constantly wear badges' as a design property that is expressed as *Control Points*; *Control Points* capture the number of places where identity is required to proceed with some action. The exposure of the identity to the rest of society is captured by the code *Identity Exposure*; this property expresses how much control an individual has in the presentation of the identity to the rest of society. Finally, the small set of individuals enrolled in the system is captured by the concept of *Population Participation*; the ratio of individuals enrolled into the system to the rest of the population that are not enrolled.

The codes have been developed to express a measure of the amount of relevant affordances that the system can provide for each property. Therefore, the Poor Laws with the badges would have a high number of *Control Points*, a high degree of *Identity Exposure* and a low level of *Population Coverage*. It is the interaction of these design properties that brings about the feelings of shame that were identified as the cause of rejection.

Further analysis of all the codes, revealed that the design properties can be distinguished into two main categories: structural properties and the metrical properties (see Table 3). Structural properties focus on the design aspects that capture the flow and relationship of an individual's information within the identity ecosystem created. Metrical properties are based on the qualities that are affected by the type and amount of information that is being collected and used in the identity system.

Setting the context

In this section, we introduce two identity systems that were used in the thematic coding process—UK DNA Database and the Austrian Citizen Card. An outline of the basic implementation details and the eventual outcomes is provided for both identity systems. This section does not touch on any of the properties that have been uncovered, but serves as a base for contextualising the properties when they are introduced in the following sections. Doing so is useful, as it allows the later introduction of each property to be discussed and elaborated upon within a particular context.

Table 3 System properties

Structural properties	Metrical properties
Control Points	*Population Comprehension*
Subject Engagement	*Expert Interpretation*
Identity Exposure	*Information Accuracy*
Population Coverage	*Information Stability*
	Subject Coupling
	Information Polymorphism

The UK criminal DNA database is an identity system consisting of a central database that stores an individual's DNA sample, and creates an identifier by analyzing 10 different regions of randomly repeating DNA sequences (Short Tandem Repeat Sequences) that differ among individuals (Parliamentary Office of Science and Technology 2006a). Such systems are typically accessed by law enforcement agencies to identify suspects, by matching crime scene DNA samples to those in the database. The DNA database can be considered an extreme form of identity management. For example, DNA identification has become a highly deterministic in that judgements are made solely on DNA identification—irrespective of other evidence—even though experts warn of the dangers this harbours (2009). The system contains not only the DNA of convicted criminals, but of all suspects, and persons who gave DNA for purposes of being eliminated from an investigation. There has been a public debate on the way in which the system is operated, and legal challenges which resulted in a recent ruling that the system violates *Article 8* of the European Convention of Human Rights (BBC 2008b).

The second identity system covers digital identities in an online environment. Austria is regarded as a leading implementer of e-government among the European countries. To facilitate its vision for the provision of online services, the government concluded that it required a system to support the identification and interaction of services in a digital environment. The concept of the Austrian Citizen Card was defined to fill this role (Leitold and Posch 2004). Even though the name 'Citizen Card' suggests otherwise, it is not a single physical card—rather, it is a concept for a set of standards and requirements that have been developed to support digital identification and authentication (Arora 2008). The Citizen Card outlines mechanisms for secure digital identity and digital signatures. Individuals can obtain Citizen Cards from a number of providers. For example, digital signatures are automatically loaded onto official government eCards, where individuals will need to voluntarily activate the digital signatures in order to use it. Alternatively, individuals can choose to load and activate the digital signatures onto Bank ATM cards and even mobile phones (Meints and Hansen 2006).

Rollout of the Austrian Citizen Cards to the entire population was completed by the end of 2005, but by early 2009, only 74,000 individuals had activated their digital identities and signatures (Martens 2010). This represents 0.9% of the overall Austrian population, with a very slight increase of about 0.2% from the year ending 2005 (Meints and Hansen 2006). A-Trust, an Austrian certification service provider, attributes the lack of adoption to the complexity, cost and lack of benefit from an individual's point of view (Sokolov 2006a, b).

Structural properties

This section introduces the structural properties of the framework. Each individual property will be applied to the UK DNA Database and the Austrian Citizen Card contexts (see "Privacy"). The structure of an identity system refers to the manner in which an identity ecosystem is constructed—these are key choices system owners and designers can make about the identity system, which directly impact an individual's lived experience. These properties seek to capture the flow of information inside the web of identity that is established. The structure of an identity scheme will define how the interaction between individual and society is

shaped by the identification system, affecting the possible outcomes that an individual will face.

Control Points

One of the main structural properties of any identity system can be expressed in terms of the number of *Control Points*, which represents the situations in which an individual's identity is required in order to proceed with a particular function. This includes situations where identity and personal information are being consumed for the purpose of identification and authorisation, as well as situations where the information is being captured for the purpose of enrolment or updating. A simple example would be the need to show proof of age when purchasing alcohol. Without the proof, the individual would not be able to proceed with the purchase. When an identity ecosystem contains a large number of *Control Points,* the identity is frequently accessed by the relying party. A low number of *Control Points* implies that an individual's identity is not used or requested frequently.

In the context of the DNA Database, each time a DNA sample is extracted from a crime scene or taken from an individual it is checked against every single identity entry in the database. According to the official statistics (National Policing Improvement Agency 2010) in 2008/09, a total of 14,452 crime scene samples have produced a match from the DNA database, with a total of 410,589 matches since 1998. This means that every single identity within the system has been accessed, at the very least, 14,452 times in 2008/2009—a high number of *Control Points*. In contrast, the Austrian Citizen Card system is designed as a voluntary system to support eGovernment services. However, the average number of interactions between individuals and the public sector has been roughly estimated to be "*1.7 contacts per year*" (Aichholzer and Strauß 2010). This represents a low number of *Control Points*. Furthermore, for a majority of these online services can be accessed without the use of an Austrian Citizen Card (Aichholzer and Strauß 2010). As the Citizen Card does not have to be used in these contexts, they are not true *Control Points*, further reducing this number.

How does the number of *Control Points* affect the *lived experience*? A high or low number of *Control Points* in itself is not positive or negative. A high number of *Control Points* in the DNA database implies that an individual's identity is constantly being accessed. This means the DNA Database becomes a surveillance tool that authorities use to deter individuals in the database from committing crimes (2007; Science and Public Protection 2009). Situations where individuals are "constantly watched" can create feelings of paranoia, which can limit individual freedom. The low number of *Control Points* in the Austrian system indicates a lack of opportunity to make use of the identity, creating perceptions that there is little benefit in using the system (Aichholzer and Strauß 2010).

Subject Engagement

This property captures whether an individual is an active or passive participant in the use of the identity. A system with a high level of Engagement gives individuals an active role in the presentation of their identity, usually meaning an individual needs

to be present, or is at least aware, when their identity is used. On the other end of the spectrum, individuals can be completely passive members of an identity scheme. Systems with a centralized database that stores information usually have low levels of *Subject Engagement*, as records stored on the database can be accessed by the organisation without the individual being present, and be unaware that the identity is being accessed.

Forensic criminal identification systems—by their nature—do not directly involve individuals, because there is an assumption that criminals will attempt to evade authorities if they are aware that they have been identified as suspects of a crime. The DNA database is no exception; an individual is only involved during the initial DNA collection, and following positive identification. Any other access of the information happens without the individual's involvement or knowledge. Therefore, as an individual assumes a very passive role, the DNA database has a low degree of *Subject Engagement*. In contrast, the Austrian Citizen Card is a voluntary system that requires individuals to take initiative in the activation and use of their digital signature (Aichholzer and Strauß 2010). It has a high degree of *Subject Engagement*.

If there is a low level of *Subject Engagement,* individuals may not be aware when their identity is being used. This can create concerns about who might be accessing the identity, what they may be doing with the information and the consequences this might have for the individual. In the case of the DNA Database, DNA profiles have been handed out to private firms for research purposes, such as the development of familial searching (identifying relatives through DNA), without the respective individual's knowledge (Hope 2008). A high level of *Subject Engagement* minimises this risk for privacy invasions, but introduces the possibility of the system becoming an unacceptable burden for an individual, as he or she is now required to exert effort to make use of the identity. The activation process for the Austrian Citizen Cards is cumbersome. The actual usage of the digital signatures has a high learning curve, and problems can still occur during use (Aichholzer and Strauß 2010). Therefore, the system requires a large amount of effort in relation to the potential benefits, helping to explain the resistance in the form of non-adoption of the system.

Identity Exposure

An individual is typically enrolled into an identity system to determine his/her respective rights, privileges and/or the necessary course of action—this involves the presentation and use of individual identities at various *Control Points*. The process of the identity being accessed and used by a relying party carries with it the risk of the identity being exposed to other, non-reliant parties. Uncontrolled disclosure of information can be expressed as the degree of *Identity Exposure*; it refers to the degree of control that individuals have over the presentation of his/her identity to the rest of society, highlighting issues around social perceptions, values and acceptance of such identities. A system with a high degree of exposure constantly reveals the identity information to third parties that have no rights or permission to obtaining the identity. Identity systems that allow an individual to preserve the integrity of the identity from other parties have a low degree of *Identity Exposure*.

In the case of the DNA database, individuals have no control over the presentation of their ("criminal") identity to the rest of society. This is especially

true in connection with serious crimes, where a positive DNA match is seen as an indication of guilt, and can trigger a man-hunt via media channels. The Austrian Citizen Card has been designed as an identification and authentication mechanism, and therefore does not provide the identity of the individual to anyone but the relying parties the individual is interacting with. The use of sectoral identifiers—which are unique identification numbers that differ within different contexts of use—further protects individuals from exposure; there are 26 sectors (such as tax, health, education, etc.) that each use a different identifier per individual. This prevents the connection of different identities across separate contexts (Aichholzer and Strauß 2010).

A high degree of *Identity Exposure* potentially means an individual cannot evade judgement by third parties based on the revealed identity. Shortly after the European Court ruling on the database being a "*breach of rights*" (BBC 2008b), a police chief at the time defended the database stating that *"the public expectation now is that crime will be solved, not by the presence of witnesses, but because there will be DNA..."* (O'Neill 2008). Although not a directly associated with the UK DNA Database, the events following the disappearance of Madeline McCann in Portugal illustrate public perceptions of the connotations of a DNA match. When Madeline's DNA was found in the boot of the car that her parents had hired, initial sympathy over the disappearance of their daughter quickly turned to "*defamatory comments*" because the presence of DNA was seen as proof of their involvement in her disappearance (The Independent 2007). A low degree of *Identity Exposure* means there is a low risk of uncontrolled exposure of an individual's identity. In the Austrian Citizen Card Scheme, an individual's digital identity and signature is loaded onto his/her personal device, such as the government eCard. The device and therefore, the identity is under the individual's control ensuring that the identity doesn't leak out without the individuals knowledge (Leitold et al. 2002). Furthermore, the use of the identity takes place in a digital medium that makes use of encryption and secure digital channels for communication. This provides the system with a low degree of *Identity Exposure* ensuring that the individual remains in control of the identity.

Population Coverage

Population Coverage describes the number of individuals that are registered in and interact with the system, in relation to the size of the total population (which are not enrolled in the system, but are still able to act in the context of which the identity system operates). A system with a low level of *Population Coverage* would be highly targeted—the number of individuals that are registered on the system consists of a small part of the entire population that are able to act in that context. On the other hand, a system where all or most individuals are automatically enrolled has a high level of population participation.

While the UK DNA database is currently the world's largest DNA database, it holds about 4.8 million individual DNA samples; representing only 7.39% of the total UK population (Hayles 2009). This implies a low level of *Population Coverage*, i.e. a highly targeted form of identification. In contrast, the Austrian Citizen Card system was designed as a universal identity scheme. Given that the eCards has been distributed to the entire population, it has a high level of *Population Coverage*.

Low levels of *Population Coverage* can be linked to issues of discrimination. Individuals are identified simply by being part of the system—and are more likely to be unfairly scrutinised by authorities in comparison to those who are not. In its review of the UK DNA Database, the European Court of Human Rights has ruled the retention of the DNA of un-convicted individuals as unlawful (BBC 2008b). Significantly, the inventor of DNA fingerprinting, Sir Alec Jeffreys, has called for DNA of non-convicted individuals to be removed stating that "*there is a presumption not of innocence but future guilt"* (Whitehead 2009). There are also systematic biases in terms of population selection—the DNA of 40% of young black males is in this database—which led a judge to suggest that all citizens' DNA should be captured (Orr 2007; BBC 2007a). The Austrian Citizen Card has a high level of *Population Coverage*. The universality of the system over the entire population, removes the possibility of distinctions being made against those who are enrolled against those without an identity. Therefore the issue of possible discrimination based on the enrolment into the Citizen Card scheme has been eliminated.

Metrical properties

This section introduces the metrical properties that were coded in the thematic analysis. Each metrical property will also be discussed within the context of the UK DNA database and the Austrian Citizen Card (see "Privacy"). The metric of an identity system refers to the techniques, methods and technologies that are used to capture and present an individual's identity. The metrical properties defined here capture the implication that the type of information has on the lived experience of the individual.

Expert Interpretation

The first metrical property is the level of *Expert Interpretation*, which captures the amount of human activity required to collect and use identity information. Systems with a high level of expertise require specially trained staff to handle the identifying metric at various stages throughout the lifecycle of the identity. Systems that require a high level of *Expert Interpretation*, as opposed to systems where anyone can interpret the identifiers, involves subjective judgements, where the determination of identity depends on the examination of information by human experts. Automated systems serve to decrease the amount of expert analysis involved, providing systems with an objective approach to processing identity.

DNA identification works by matching specific DNA markers obtained from two separate samples (Parliamentary Office of Science and Technology 2006b). If the two samples contain all of the same markers, a match is made (positive identification). Specific equipments are required as part of this process, but it is not an automated one, as several steps require interpretation to determine if there is a match. The decisions to ignore, accept or to reason about the absence or presence of certain markers brings a degree of subjectivity into the identification process, creating a system with a high degree of *Expert Interpretation*. On the other hand, digital signatures are built on mathematical models of encryption, offering an implementation that is completely objective and automated. The process of identification does not require human beings

to interpret an individuals identifying or authenticating information. Therefore, the Austrian Citizen Card system has a low degree of *Expert Interpretation*.

A high degree of *Expert Interpretation* implies a reliance on subjective decisions about an individual. It creates a non-transparent situation, where non-experts cannot assess the reliability of the identification process, leading to an assumed infallibility of the expert decisions. This leads to the possible implication that an individual can be wrongly identified, and in the case of a criminal system he/she might be wrongly accused of a crime. The 1993 case of Timothy Durham in Oklahoma (W. C Thompson et al. 2003) illustrates the potential consequences of such mistakes. Timothy Durham was found guilty of raping an 11 year old girl, based on the alleged victim's eyewitness identification, a hair sample from the scene that was similar to Durham's hair, and most importantly the DNA test of semen—which matched Durham. The guilty verdict was passed despite 11 witnesses placing Durham in Dallas at the time of the rape. Durham was eventually set free in 1996, after further testing revealed that the semen could not have come from him and highlighted the error in the initial DNA test that *"arose from misinterpretation"* (W. C Thompson et al. 2003). A low degree of *Expert Interpretation,* such as the Austrian Citizen Card, eliminates the risk and the dangers of subjectivity as the identification process is an objective process free of human error. Objectivity creates a predictable process that provides a level of transparency in assessing the correctness of identifications.

Population Comprehension

Another metrical property is the general level of understanding that the population at large has of the techniques and technologies used for identification. In a system with a low level of *Population Comprehension*, citizens have little to no knowledge on how the metrics are used to identify them. This typically happens when a large number of the general population cannot interpret the significance of an identification being made, why it may be wrong, or how the identity system works. On the other hand, systems with high levels of understanding are those in which an individual has a good mental representation of the entire process in which the identity metrics are used.

Whilst there is a high level of awareness that DNA is used for identification, most individuals do not understand the process by which identifications are made, nor can they easily grasp the implications behind the probabilities attached to DNA matching—such as a "*one in trillions*" probability of a chance match occurring between two unrelated individuals (E. Graham 2007). A recent study (Ley et al. 2010) found that perceptions of the entire DNA process have been shaped by a "*CSI effect*", in which the inaccurate media portrayal of DNA applications has distorted perceptions of the entire identification process. As such, the DNA database has a low level of *Population Comprehension*. Similarly, the Austrian Citizen Card also suffers from a low level of *Population Comprehension*. Digital Signatures are not a technology that is easily understood by laymen (Garfinkel et al. 2005a). A study of merchants trading through Amazon (Garfinkel et al. 2005b) found that only 54% of those understood how the digitally signed receipts they were receiving worked. 59% of merchants thought it was important to use encrypted and signed mail, yet 59% also admitted to not knowing whether their eMail client supported it.

Low levels of *Population Comprehension* indicates the possibility that individuals cannot challenge identification decisions, as people in general do not understand how the information is processed, nor do they know how to interpret related figures. In the case of Madeleine McCann (see "*Identity Exposure*"), traces of her DNA was found in the boot of the car hired by her parents. For many people reading this in the press, and members of the Portuguese police, the presence of Madeleine's DNA implicated her parents (Rayner et al. 2008). However, DNA can be easily transferred via her clothes and toys that had been transported in the boot. Another issue brought by low levels of *Population Comprehension* arises in voluntary use systems. If individuals do not understand how to use the identification technologies, such as digital signatures, they may not be able to identify themselves when they need to, and/or be fooled by fake credentials. In this context, the low levels of *Population Comprehension* can indicate potential confusion on how to make use of the identity and therefore the system. This can be linked to the issue of complexity that has been raised in the Austria Citizen Card scenario, contributing to the situation where individuals are not using the digital signatures resulting in low rates of adoption (Sokolov 2006a, b).

Information Accuracy

Information Accuracy is the property that defines the reliability of the information that is collected, stored and used in the identity system. Systems with high degrees of *Information Accuracy* are more likely to produce correct identifications. However, this accuracy must not be based solely on the theoretical possibilities—accurate "measurement" of *Information Accuracy* needs to take into account the implementation specific details that can affect the theoretical probability. The inconsistencies and practical limitations of the real world will need to be reflected in the *Information Accuracy* property of the system.

DNA identification can offer high degrees of accuracy if the samples being compared are of high quality (Graham 2007). In law enforcement, however, DNA samples are not only collected from individuals, but also from the crime scenes. Such samples may be contaminated by other DNA present at the scene, or might have degraded over a period of time before it is captured and stored. Although it is difficult to measure the effects of contamination or degradation, it is important to note that this decrease in the degree of *Information Accuracy* reduces the probability of a correct identification being made (Thompson et al. 2003). Austria's Citizen Card scheme offers a high degree of *Information Accuracy*. The system is designed around unique identification numbers and digital signatures that are issued to each individual in the population (Leitold et al. 2002). If implemented correctly, the use of digital signatures should leave no doubt as to its authenticity.

The impact of a low degree of *Information Accuracy* on the lived experience is that individuals are at risk of false positives (falsely matching someone to a DNA sample), resulting in individuals being wrongly accused. In the recent case of the Omagh bombing, the judge called into question the reliability of the Low Copy Number (LCN) DNA identification technique, which makes use of minute DNA samples for matching purposes (2007). The merit of the technique is still being debated in the scientific community (Graham 2008). As a result of the case, the

police suspended the use of the LCN technique, which up to that point had already been used in 21,000 different cases (Hope 2007). In the case of Timothy Durham see "*Expert Interpretation*". (Thompson et al. 2003), the misinterpretation of the DNA was a result of the failed separation of the contamination between the male and female DNA during extraction of the semen stain. When an individual first activates an Austrian Citizen Card, an "*identity link*" is created based on unique citizen identification (H. Leitold et al. 2002). The identity link also contains name, date of birth, and an individual's public key that is used to support digital signature functions. This identity link is then digitally signed by a government authority, which prevents tampering, and provides high levels of assurance that the identification information held on the card is accurate—minimizing the danger of erroneous identification of an individual caused by inaccurate information.

Information Stability

The chosen metric for an identification system will also have an impact on the stability of the registered identity. *Information Stability* refers to the rate with which the information stored in an identity system changes over time, and thus supports reliable identification—long after it was first recorded. A system with low *Information Stability* means the identity information has the potential to fluctuate greatly over short time frames. Identity systems that make a large use of biographical information typically have low levels of stability as the information can potentially change at any given time (e.g. address, profession, etc.). Some biometrics can seem to be stable over the lifetime of an individual (e.g. iris), whereas others change over time, or can be altered by the individual (e.g. face recognition).

An individual's genetic makeup does not change over time, and offers a high degree of "*permanence*" (Jain et al. 1999). This means that regardless of the time between collection and identification, an individual's DNA sample will always produce a match with that particular individual. As such, the DNA database offers a high level of *Information Stability*. The information used to establish an individual's identity in the Austrian Citizen Card scheme (i.e. identification number, name, date of birth and public key) does not tend to fluctuate greatly over time. For example, an individual cannot change his/her date of birth, and is usually tied to a single identification number over a lifetime. Therefore, the Austrian Citizen Card has a high level of *Information Stability*.

A high level of *Information Stability* potentially threatens individual freedom, as an individual is unable to redefine his/her personal identity to evade detection if the DNA is used for different purposes. Austrian Citizen Cards also have a high level of *Information Stability*, and are subject to the same potential issues. Even though an individual can change his/her name or be issued with a new public key, the unique identification number and the centralization of such change processes allows the government to maintain a link of the "new" identity to the original identity that was first created.

Subject Coupling

Identification systems do not only vary in terms of the stability of the information collected, but the amount of information that is collected and used for a particular

purpose. This property of the system is known as *Subject Coupling*, i.e. the degree of representativeness between the captured identity and the relevant "*partial identity*" (Pfitzmann and Hansen 2008) of the individual in relation to the purpose and context. A tight coupling suggests that the captured identity metrics faithfully represents an individual's partial identity at the various *Control Points* that it is applied. On the other hand, a system that collects too much or too little information about an individual is said to have a low *Subject Coupling*, since the identity that is captured and presented does not accurately represent the 'complete' individual in that situation. While this property may seem like an easy aspect to establish, ensuring that *Subject Coupling* is accurately assessed depends on more subtle nuances about the information around the identity and the context.

While a lack of information to represent an individual means that there is a low *Subject Coupling*, the inverse is not always true. *Subject Coupling* occurs when the identity created does not represent the individual in the context. Collecting 'too much' information also results in low levels of *Subject Coupling*. When too much information is known about an individual, the consumer of that identity might then judge the individual based on information that is not relevant for the particular purpose (Fig. 2). An example of having too much information would be the use of branding to enable authorities to identify recidivists (Caplan and Torpey 2001). When released, the physical marks were clearly visible to everyone, all the time. This removed any chance of re-integration into society.

Consideration of this property requires designers and implementers to account for an individual's own perception of the relevant partial identity. As such this property should not only be considered from the organisations point of view, but must also consider how each individual perceives their role with respect to the organisation. The focus is on the relationship between the individual and the implementer, influencing the information that the individual assumes is relevant to the instantiated identity. Therefore, *Subject Coupling* must also ensure that there is a good mapping between the individual's perception of the relevant identity and the organisation's perspective of the relevant identity.

The DNA database is meant to identify people connected to crime—either to pursue further investigation, or to eliminate a potential suspect from it. If the identity is limited to just the elimination of suspects, the system would have a high degree of *Subject Coupling*. However, the faith that many individuals put into such systems means DNA has become a highly deterministic form of identification: a positive DNA match can greatly influence the perception of an individual's identity, causing other relevant information to be discarded or distorted in light of the match. Furthermore, in relation to keeping DNA of non-convicted individuals, a recent report from the Home Office (Science and Public Protection 2009 has stated that the "*risk of offending following an arrest which did not lead to a conviction is similar to the risk of reoffending following conviction.*" This can be interpreted as an assumption of guilt through association with the DNA database, where the view becomes that "*innocent people who have been arrested are more likely to commit a crime*" (Goldacre 2009). The system can therefore be said to posses a low level of *Subject Coupling.* The Austrian Citizen Card system is designed as a digital identification and authentication scheme. Its purpose is to provide individuals with mechanisms to securely and accurately identify themselves to other organisations.

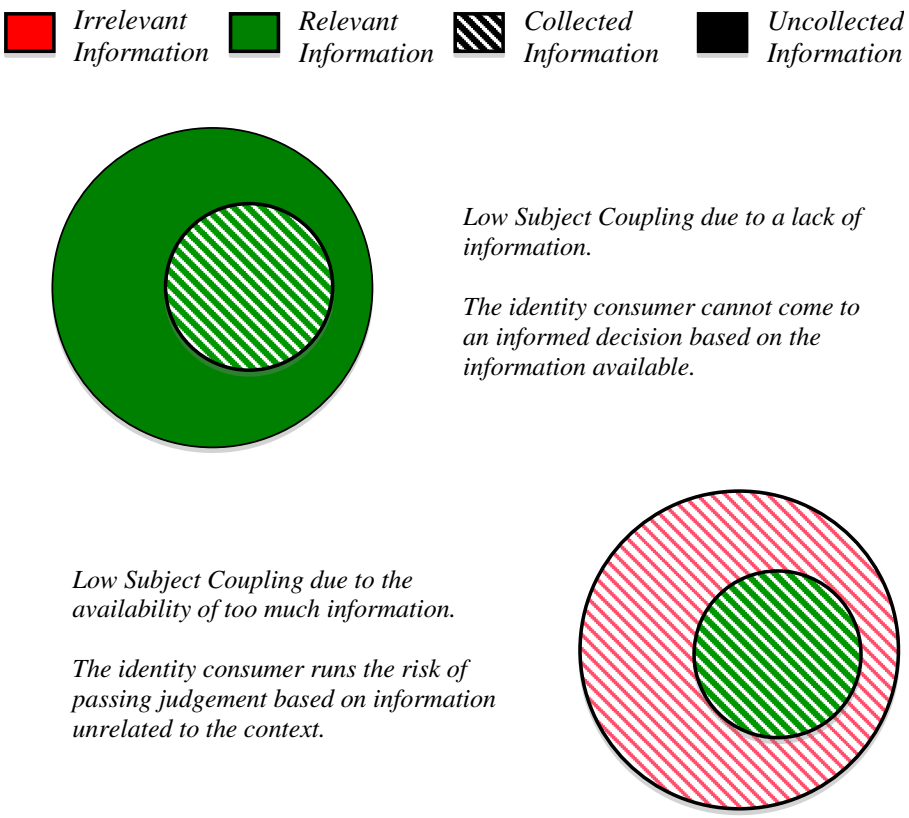


Fig. 2 Low levels of *Subject Coupling*

Therefore, the identity link created, based on the unique id number, the name, the date of birth and public key (H. Leitold et al. 2002), seems to fit its purpose and does not collect or make use of other information beyond what is needed. It provides a high level of *Subject Coupling*.

A low level of *Subject Coupling* indicates the potential dangers where individuals may be judged on an unrepresentative form of identity. Raymond Easton was charged with burglary when his DNA sample was matched to a crime scene (BBC 2007b). However, Mr Easton was in advanced stages of Parkinson disease, and could not have committed the crime. While he was eventually released and the charges dropped, this only came after an advanced DNA test was made. In a separate case from 1997, George Ellis was sentenced to 14 years in prison for robbery (BBC, 1999) Despite claims that it was planted, he was convicted solely on the DNA evidence. Two years later, criminal charges were brought against detectives involved in George Ellis's case, calling into question the validity of the DNA evidence. An appeal court came to the conclusion that it could not uphold the conviction since the "*DNA evidence was the most damning piece against him*" (1999). As such, having a low level of *Subject Coupling,* the DNA database introduces situation where decisions to be made based solely on the positive DNA match. Offering a high level of *Subject Coupling*, individuals in the Austrian Citizen Card system are not unfairly

judged based on the identity created. The information used in the scheme is sufficient just for purpose of identification. Its use in different contexts (health, tax, etc.) will then be supplemented with other personal information that will need to be collected and stored by each relying party, whose information systems remain independent of the Citizen Card system (H. Leitold et al. 2002).

Information Polymorphism

Depending on the chosen metric, an individual's identity may be more or less likely to being used for different purposes. The likelihood that the identity may be used for a different purpose increases with the various meanings that can be attributed, extracted or interpreted from the type of information held about individuals. This is captured by the term *Information Polymorphism*. This property is derived from the quality of the information itself, and therefore needs to be assessed irrespective of any laws that are put in place to prevent such abuse of the collected information. Such safeguards are easily circumvented, especially if the required information has already been collected and stored. In systems with a high level of *Information Polymorphism*, an individual's identity information can be easily taken out of context of the original scheme, and applied to other systems that use this information for different purposes. Such systems are more likely to lead to what is commonly described as *function-creep*. A low degree of *Information Polymorphism* means that an individual's identity is safe from being exploited for other functions.

DNA can be used not only for individual identification purposes, but also for a number of other purposes such as identifying racial heritage and familial linkages (paternity), or the likelihood of developing certain illnesses. The DNA database therefore has a high level of *Information Polymorphism* since information can potentially be used for completely different purposes. The identity created in the Austrian Citizen Card system relies on information that does not lend itself to various uses. For example, the public key can only be used to support authentication or digital signing procedures. Furthermore, each service that an individual interacts with will make use of different sectoral identifiers preventing the combination of information across various contexts (Meints and Hansen 2006), reducing the possibility of information being joined together for other purposes. The Austrian Citizen Cards therefore offers a low level of *Information Polymorphism*.

A high level of *Information Polymorphism* potentially threatens individuals' privacy. The DNA stored in the UK DNA database is currently governed by law that states it can only be used to investigate crime. However, the Chief Constable in charge of the database regularly receives requests for matching to be performed for paternity cases; even though these are refused, the risk of paternity suits has been cited as a reason why police officers do not want their DNA to be stored for elimination purposes (Bennetto 2000)—something that is done with fingerprints. Furthermore, there is the issue of unpredictable future governments and how they might potentially change laws around the collection and use of DNA information. For example, when the DNA Database was first implemented in 1995, the law stated that only the DNA of convicted individuals would be stored in the Database. This was later changed when the Criminal Justice and Police Act 2001 allowed the government to collect and store DNA of non-convicted individuals.

At first glance, the use of unique identification numbers in the Austrian Citizen Cards might imply a high level of *Information Polymorphism*, as these identification numbers typically allow for the linkage of information across different contexts of use. Unique identification numbers allows for the creation of detailed user profiles that can invade an individual's privacy. For example, (Lyon 2003) mentions how insurance companies in the United State use increasingly intrusive methods to collect personal information based on an individual's Social Security Number. The Austrian Citizen Card has been designed to minimise risk, by creating unique sectoral numbers. In a particular context of interaction, the unique identification number goes through an irreversible cryptographic hash to produce a new sectoral identification number that is then be used to identify the individual within that particular context (H. Leitold et al. 2002). This prevents an individual's identity from being linked up across different contexts, containing an individual's information to use within each scenario. This creates a low level of *Information Polymorphism*, minimising the possibility of privacy invasions and function creep.

Combining properties

Looking at the various properties individually—as we have in the preceding sections—can help researchers and practitioners to understand the possible impact of an identity system on the lived experience. In certain configurations, such as an identity system a high number of *Control Points*, the system might be perceived as being—'too controlling', and would thus might be met with resistance. A system that needs to be up-to-date, but makes use of a metric that has a low level of *Identity Stability,* may be seen as a burden upon individuals, who continuously have to report when information changes.

However, reactions to identity systems are rarely brought about by any single property alone. It is the combination of these various properties and their interactions that allows for the proper assessment of the lived experience. In doing so, one can then construct the possible narratives and therefore the potential outcomes while paying attention to the various contextual elements and social norms. For example, consider a system with a low level of *Population Coverage*, a high level of *Subject Engagement*, and a high number of *Control Points*. The resulting identity system is a highly targeted one, indicating that certain criterion needs to be met for inclusion into the system. The majority of the population that is acting in that particular context is able to bypass the system. Additionally, as individuals play an active role at a large number of *Control Points*, some might decide that the burden of the system is unbearable. As such, in cases where it is possible to do so (e.g. identification systems based on religion), one can analyse the situation and deduce that a number of individuals might avoid the identity system altogether, by abandoning his/her 'identity' and constructing a new one.

With the Austrian Citizen Card, there was lack of adoption and use of the digital signatures (Sokolov 2006a, b). Putting the system in the context of the properties, we can link the low uptake of the system to the low benefit for individuals, as there are few instances where they can make use of their identity (low number of *Control Points*), and the fact that digital signatures are not understood by many people (low levels of understanding), As such, being individuals that play an active role (high level of *Subject Engagement*), they are not motivated to make use of their digital signatures.

For the DNA database, most of the properties introduced here are relevant to interpreting the various reactions towards the system. The initial set of privacy concerns stem from the constant access of the identity (high number of *Control Points*) of which the individual is unaware (low levels of *Subject Engagement*). This is further amplified by the possibility that the identity information can be easily reused for other purposes in completely different contexts (high level of *Information Polymorphism*), again potentially without the individual being aware.

Issues of fairness and freedom also come into play when considering the highly targeted nature of the DNA database (low level of *Population Coverage*), especially in light for the lack of control that an individual has over the presentation of the identity to the rest of society (high level of *Identity Exposure*). Furthermore, the lack of control is substantially worsened by the incomplete yet deterministic nature of such identification (low degree of *Subject Coupling*), that takes places in a subjective process (high levels of *Expert Interpretation*) based on potentially inaccurate information due to contamination and degradation (low levels of *Information Accuracy*).

Based on this narrative for the DNA database, it is not surprising that the system is surrounded by privacy concerns and controversy. These concerns are given strength, perhaps non-intuitively, by the broadening of the *Population Coverage* as it includes not only convicted criminals but suspects as well. This can perhaps be explained by the fact that it is still a highly targeted system, just slightly broader in scope, Additionally, from the point of view of innocent suspects, they do not belong on the database at all, meaning the partial identity created goes against the relationship between the individual and the state, thus further driving down the level of *Subject Coupling*.

Applying framework to non-government identity systems

The system properties introduced in this paper were developed through an investigation of past and present National Identity Systems, and we have explained them in the context of two such schemes. To illustrate the applicability of the properties to different contexts, the properties will be used to investigate identity and information systems that have been implemented in completely different environments. In the following, we apply the properties to a social networking system, and a personalized advertising platform.

Social networking

Online Social Network Sites (SNS) have experienced significant growth over the past few years. It has become an increasingly popular medium for individuals to connect with each other and share a high degree of personal information. From our point of view, an SNS can be viewed as an Identity Management System. This makes such sites a prime candidate by which we can apply the codes that the research has uncovered. Specifically, we will be looking at the Facebook platform.

With over 200 million registered individuals, Facebook is arguably the most popular social platform today. It has also been the centre of some controversies. Just recently Facebook has been accused of breaching Canada's Privacy Laws (BBC

Table 4 A brief analysis of systems used in thematic coding

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
Poor Law Badges	***High***	***High***	***High***	***Low***	***Low***	*High*	*Low*	*Medium*	*Low*	***High***
	Few people came forward to request for an identity. *Beggars were required to prove that they could not get work. They were required to wear badges at all times in order to prove that they have the right to request for alms.* *A small number of individuals had to constantly wear badges on their arms, which were clearly visible to everyone else. This shamed individuals, making them unwilling to come forward.* *Furthermore, the information was also to determine parenting ability, a purpose that differs from the original.*									
Criminal Wanted Lists	*Low*	*High*	*High*	*Low*	*High*	*High*	***Low***	***Low***	***Low***	*Low*
	High rates of evasion. *The system is based on a simple set of physical descriptions that had a focus on the attire of individuals. This data was not very accurate and involved a high degree of subjective decisions as to a match. Furthermore the individual can easily change his physical appearance by donning disguises or new attire.*									
Russian Internal Passports	*High*	*High*	*Low*	*High*	***Low***	*High*	*Low*	*Low*	*High*	*Low*
	Large number of evasion attempts and manhunts were frequently launched. *The identities created tied individuals to a piece of land where they were required to work. This identity was rejected by individuals who did not agree with the relationship and attempted to flee from the state.*									
French 1912 Law	***High***	***High***	*Medium*	***Low***	*Low*	*High*	*Low*	*Medium*	***Low***	*High*
	Part of the targeted population (Romani) abandoned their way of life and assumed new identities. *The system was a burden on individuals, constantly showing their identities when ever they moved. Being a highly targeted system, an individual can avoid the system by "changing" his/her identity.*									
French Bertillonage	*Low*	***High***	*Low*	*Low*	*High*	*Medium*	***High***	***Low***	***Low***	*Low*
	Reliability and effectiveness of recidivists was called into question. *The identification process was highly subjective using inaccurate information, resulting in inconsistent identifications. As individuals were involved in the identification process, they could alter their dimensions by not fully co-operating, e.g. not standing straight, etc. Furthermore, it was ineffective at identifying young individuals as they were still growing.* *In Argentina, system was rejected on grounds that the measurements insulted their honour. It can be argued that they either did not understand the process or they felt that it was a misrepresentation of their identity.*									

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
Argentina Dactyloscopy	*Low*	*Low*	*Medium*	*Low*	*Medium*	***Low***	***High***	***Medium***	***High***	*Low*
	Dactyloscopy has become a de facto standard in criminal investigations. *Fingerprints collected did not change over time and was more accurate than body measurements or descriptions. It gave the identification of criminals a form of "mechanical objectivity" in that the fingerprints were captured using objective approach.* ***Issues of false accusations have recently been called into question.*** *Dactyloscopy still requires subjective decisions to decide if there is a match. Crime scene fingerprints are not accurate representations of fingerprints, further raising the error rate. People are not aware of the entire fingerprint identification process and therefore individuals lose the ability to resist such accusations.*									
WW I and II UK Identity Cards	***High***	***High***	*Low*	*High*	***Low***	*High*	*Low*	*Medium*	***Low***	*High*
	Individual information was out of date. *The information collected included attributes such as address which were open to change. The high variability in the information collected and stored, required the co-operation of individuals to update their records as needed. The public however proved unwilling to assist the in these procedures, especially since the cards did not provide any benefits after war time (after its use in food rationing). It is perceived as the needless prussianzing of institutions.* ***Resistance to carrying and showing ID Cards.*** *The needs for identity cards represent a clash in the culture for the public. The identity created by such a system goes against the relationship that exists between the state and its people. Therefore, the identity instantiation did not match well to the individuals' perception of the situation. This led to resistance towards hosing ID cards, as in the case of Wilcock, which was brought to court and gained a lot of public support and negative media publicity against the ID cards.*									
WW II Nazi Jewish Identity System	***High***	*High*	***High***	***Low***	***Low***	*High*	*Low*	*High*	*High*	***High***
	Paralysis of the Jewish Population. *The identity system created was highly targeted to the Jewish population. It started of as an identity document with clearly stated markings, indicating the individual was a Jew. This eventually led to the use of symbols that had to worn and be visible at all times. This made the Jewish directly visible to the other members of the population limiting their freedom and movements* ***Aid in the mass killings.*** *The biographical information used in the system, lends itself to other purposes. In this particular case, it made it easy to gather and round up the Jewish population aiding in the act of genocide.*									

Table 4 (continued)

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
UK DNA Database	***High***	***Low***	***High***	***Low***	***Low***	***Low***	***High***	***Medium***	***High***	***High***
	Large amount of privacy concerns have been raised. *The DNA is information constantly being accessed without individuals being aware of it. Furthermore it is a highly targeted system that also includes non-convicted individuals. These individuals do not believe they should be on the database, crating a situation of conflict in the creation of the identity. This becomes a major concern since individuals cannot control the presentation of identity to the rest of society.*									
Contact Point	***High***	*Low*	*Medium*	*High*	***Low***	*High*	***High***	***Low***	***Low***	*High*
	Effectiveness of system has been called into question. *Recent cases, such as the death of "Baby P.", have raised doubts on the usefulness of the system. The individual's information being entered into the system is not objective and reduces the accuracy of the data collected. Furthermore, interpretation of results is highly subjective. As the "Babpy P." case shows carers were all aware of each other, but still failed to recognize the trail of abuse.* ***Issues of freedom and self fulfilling prophecies have been raised.*** *Services that make use of the information may pre-emptively judge an individual and change their modes of interaction. The individual is potentially being assessed on an incomplete picture of his/her identity based on interactions from another context. Furthermore, being targeted at children, such information is not stable and will continuously change, reducing the representativeness of the individual's identity.*									
Austrian Citizen Card	***Low***	***High***	*Low*	*High*	*High*	***Low***	*Low*	*High*	*High*	*Low*
	Low rates of adoption in the digital signature functionality of the Citizen Card. *The system does not present an individual with many opportunities to make use of the identity, creating a lack of perceived benefits. Furthermore, individuals do not understand the system making it difficult to use.*									

News 2009). More relevant to our considerations is a change that Facebook made to its website that brought out negative reactions among its community.

In 2005, Facebook introduced new features that affected the way in which information was distributed to an individual's network on the site. Prior to these changes, information that was inserted or updated on an individuals profile was only visible when another party visited his/her profile page. Facebook then added the *Newsfeed* feature, which essentially aggregated all these information changes and broadcast them to an individual's friends. This turned a process from a 'pull' operation to a 'push'. Individuals reacted against this and established resistance groups to voice their opinions. The Facebook CEO eventually responded, stating that no privacy options were taken away, and that the information was visible only to the same people who has access as before. "*Nothing you do is being broadcast; rather it is being shared with people who care about what you do*" (Hoadley et al. 2009). Nevertheless, Facebook took down the Newsfeed, and re-released it with various privacy controls.

In their study of the situation, (Hoadley et al. 2009) attributed the resistance to individuals' perception of "*information access*" and "*illusion of control*". Individuals viewed the Newsfeed as increasing the ease with which their information can be accessed by others, and the absence of controls reduced the perceived level of control that individuals had. While this point of view is certainly justified, the properties that have been uncovered here might be able to shed more light on the situation and better relate the changes in the system to the reactions.

The most relevant properties for this scenario are the *Control Points* and *Subject Engagement*. Pre-Newsfeed, information was only accessible when the individual's page was visited by another party. One can technically view this as a single *Control Point*. Post-Newsfeed, the number of *Control Points* increased dramatically; every party that the information was pushed to represents a Control Point, where the individual's information is consumed.

In addition, the Newsfeed can be interpreted as a reduction in the level of subject involvement. In the 'pull' model, visiting an individual's page was a requirement. The page is a representation of the individual on the platform, whom has spent time to create a profile that represents him/her to others. Therefore, accessing the individual's profile page can be seen as a *Control Point* that has a high level of *Subject Engagement*. The Newsfeed represents a loss of involvement, as the information is taken from the individual's controlled profile and broadcast to the other *Control Points* that individuals are not aware of or have no control over.

Targeted advertising

Targeted advertising has proved to be an extremely lucrative way to increase revenues. This form of advertising involves the tracking of an individual's identity across various services. It could be something as simple as contextual targeting (using keywords based on the content of the current page), or based on individuals' browsing history across one or more sites. These browsing histories and identification details are typically handled in a decentralized manner, making use of cookies stored on the user's computer. These tracking methods have raised issues among privacy advocates.

A recent study found that a significant number of the US population object to the tracking of behaviour. Turow et al. (2005) found that 86% of young adults reject targeted advertising that tracks behaviour across different websites. Advertisers, however, say that individuals—especially the younger generation—do not mind having their habits tracked. Recent developments in targeted advertising have taken the tracking to new levels.

Phorm is a company that developed a targeted advertising platform that is tied directly to an individual's Internet Service Provider (ISP). Every subscriber to the ISP's network is enrolled into the Phorm System. Every website that an individual visits is passed through the system, and is checked against a list of advertising categories. If a match is found, the category is marked in a cookie and stored on the user's computer. This cookie is then used to provide targeted advertisement on any websites through the use of a widget. The European Union has recently proceeded with legal proceedings in light of the controversial use of Phorm (Guardian 2009). The arguments are usually tackled from a high level law based view of privacy rights. Phorm's arguments claim that people do not understand the technology and how it works, claiming that it actually provides anonymity.

Applying the structural properties from the proposed framework, the items of interest are *Subject Involvement*, *Identity Disclosure*, and the level of *Control Points*. With every website passing through the system, Phorm presents individuals with a high number of *Control Points* resulting in a very restrictive environment for the individual. This situation is exacerbated by low subject involvement at the *Control Points*. The individual's information is taken in a covert manner, without the individual being involved in the process. Phorm also provides individuals with a high level of *Identity Exposure*. The tracked information is stored on a cookie on the user's computer. In a multi-user environment, the same computer will be used by various individuals that Phorm will not be able to differentiate amongst. When serving customized ads, the system is constantly at risk of revealing an individual's preference by presenting customized content to the "wrong" individual.

From a metrical standpoint, the properties of interest are *Subject Coupling*, and *Information Stability*. Phorm is a platform used by a user's ISP to deliver targeted advertisements. The relationship between the user and the ISP is that of a consumer paying fees to gain access to the network. This relationship calls for the sharing of certain general and financial information. This is the relevant partial identity of the individual in the subscriber role. By making use of Phorm, ISP's expand beyond this boundary by tracking an individual's habits in depth. This results in low *Subject Coupling* in the ISP-subscriber relationship. Additionally, an individual's browsing habits are constantly growing and producing a very dynamic data set that results in low levels of *Information Stability*. Therefore, in order to keep an accurate representation of the individual, large volumes of up to date records are required. This raises concerns of privacy due to the tracking nature of such a system.

Discussion and conclusion

Whilst the use of modern identity management systems has increased rapidly, the understanding of what constitutes appropriate use of identity lags behind.

The disembodiment of people from transactions has increased the perceived need to capture the identity of individuals, and developments of systems have largely been driven by what is technically feasible, and the administrative convenience of the organisations that commission the systems. Whilst the rhetoric of human-centred identity has been plentiful, little research has been carried out to understand the human experience of identity in technology-mediated interactions. This paper presents a first proposal for a set of properties to understand the need of individuals when it comes to identity systems, and what constitutes acceptable use.

Strengths and weaknesses

The main strength of framework is that it fills a gap in the current approaches to identity systems, as it links design of an identity system directly to the potential lived experience. It enhances our understating of the impact of such systems on individuals, beyond the traditional views of privacy and trust. As an example, what does it mean to claim that a system invades an individual's privacy? The problem here is privacy can mean so many things; it becomes difficult to state what the exact issue is. A typical system implementer would find it difficult to link the privacy concern to the state of system itself. However, by using these properties as a support mechanism, a researcher or practioner can conduct a proper analysis of the system, communicate clearly on the potential problem areas and suggest practical design changes to reduce the privacy concern.

Another benefit of the proposed framework is that proper use of these properties encourages the designer to immerse herself in the situation that the system will be used. Proper assessment of how each property interacts with another requires thought and reflection, looking at the system from the point of view of the individual and society that is affected by it. This is a breakaway from other methods that might take a highly administration-centric point of view, or a solution that might rely on a set of checklists, that removes a system implementer from the context. The proposed properties serve to re-embed the design process into the reality of the situation in which it is implemented.

However, the subjectivity required to fully utilize the framework can also be seen as a potential weakness. While there is an element of rating taking place, one would not be able to simply assign weights of importance to each property. Each context differs from the next and each property can play a slightly different role in relation to every other property. A high level or low level of rating for each property does not automatically indicate a good or bad outcome. There is a degree of interpretation required, and different individuals might perceive things differently, which can lead to a source of inconsistent results.

Furthermore, in its current state, the predictive power of the framework remains untested. The analysis of systems using these properties has taken place post-implementation. We are fully aware of the outcomes that a particular identity system has brought about. This hindsight proves to be an advantage, as it is easier to link known outcomes to the system properties than it is to link system properties to unknown outcomes.

Further research

The human-centred framework has been developed through a grounding of previously implemented nation-wide IDMS, and has been shown to be useful in different contexts from social networking systems to personalised advertising platforms. However, it still needs to be further tested and elaborated upon. By exposing this work to the community, we hope to be able to build a robust model that can prove to be a useful tool in the quest for human-centred identity. Potential areas for further development are provided below.

The properties of the framework here have been brought about through the analysis of a specific set of identity systems. Therefore, a continuous application of these properties to other implementations can serve to discover refinements to the uncovered properties. As an example, it may be beneficial to break down the *Control Point* property into *Read-Only Control Points*, where an individual's information is only consumed, as opposed to a *Write-Only Control Point* where the individual's identity entry is updated with new information. Another possible break down is a distinction between mandatory and voluntary *Control Points*.

Alternatively, new properties can be developed to cover design issues that were not present in the analysis. An example of a new property, and one that is currently under consideration, is that of *Information Salience*. This property focuses on the impact of certain metrics in other contexts. Religion for example is a very influential attribute and therefore has a high degree of salience. However, this *Information Salience* property might cause confusion and overlap with that of *Subject Coupling*. It is important to consider the relationship of the new property to the current properties, ensuring that there is no overlap or contradiction. Furthermore, new properties should be valid across different implementations of identity systems.

Another area for further development is the creation of a complete mapping between the individual properties and the potential outcomes that it can bring about. As an example, the analysis here has not identified how high levels of population comprehension might affect the lived experience, and therefore its impacts on the acceptance or rejection of an identity system. One could theorise, and seek proof of a situation where individuals might reject an identity system on the grounds that the population has a complete understanding of that system, thus enabling them to make more informed decisions on what may or may not acceptable. A complete mapping of the properties to potential outcomes would increase the effectiveness of the model in describing the lived experience. However, a degree of subjectivity is still needed. The mapping would only serve as potential indicators and would need to be judged in relation to the other properties, as well as the context of implementation.

Lastly, it would be beneficial to create an integrated framework that pulls in the various different approaches to create a complete human centred model. The aim of this proposed framework is not to replace the current approaches, but to supplement them aiding in a better understanding of how concepts of privacy and trust can be evaluated in terms of the system design. A comprehensive model that can be applied to various identity contexts would be highly beneficial to both practioners and researchers alike.

Conclusion

Identity is a pivotal construct in the interaction of an individual in a social space. Current approaches to designing human-centred solutions typically focus on the area of usability, privacy and trust. However, these approaches are utilitarian in nature seeking to create mechanisms that make it easier for organizations to collect an individual's information. They are abstracted from the reality of the situation in which the identity system is implemented. While these traditional approaches are important, we must be aware of their shortcomings, and acknowledge that the reach of identity beyond these realms.

It is an individual's identity that determines what he/she can or cannot do when interacting with others. Viewing identity as such extends the impact of identity beyond the point of interaction and data collection, shifting focus towards the practical impacts that identity has on an individual's life. Failure to acknowledge this effect of identity results in systems that can claim to be usable, privacy sensitive or trust worthy, but still result in systems that face rejection or systems that can have negative impacts for an individual. We need to take a step back from the identity system itself, and focus on the underlying relationships that are present in the identity eco-system. We need to consider the identity system in its context of operation, to analyse the system as a whole and determine its impacts on the lived experience. The framework proposed here aims to fill this gap, and act as a starting point for a genuinely human-centred approach to identity.

References

Adams A, Sasse M. Privacy in multimedia communications: protecting users. 2001. Available at: http://citeseer.ist.psu.edu/adams01privacy.html. Accessed 11 Feb 2008.

Aichholzer G, Strauß S. The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity in the Information Society. 2010:3. Available at: doi:10.1007/s12394-010-0048-9. Accessed 29 June 2010.

Ajzen I. From intentions to actions: a theory of planned behavior. In: Kuhl J, editor. Action control, from cognition to behavior. Berlin: Springer-Verlag; 1985.

Arora S. National e-ID card schemes: a european overview. Inf Secur Tech Rep. 2008;13(2):46–53.

Ashbourn J. Biometrics: advanced identity verification; the complete guide. London: Springer; 2000.

Backhouse J, Halperin R. A survey on EU citizen's trust in ID systems and authorities. Future of Identity in the Information Society; 2007.

BBC. All UK 'must be on DNA database'. *BBC*. 2007a. Available at: http://news.bbc.co.uk/1/hi/uk/6979138.stm. Accessed 28 June 2010.

BBC. Transcript—give us your DNA. *BBC*. 2007b. Available at: http://news.bbc.co.uk/1/hi/programmes/panorama/7040162.stm. Accessed 11 Dec 2008.

BBC, Ad system 'will protect privacy'. *BBC*. 2008a. Available at: http://news.bbc.co.uk/1/hi/technology/7280791.stm. Accessed 13 Aug 2010.

BBC. DNA database 'breach of rights'. *BBC*. 2008b. Available at: http://news.bbc.co.uk/2/hi/uk_news/7764069.stm. Accessed 9 Dec 2008.

BBC News. Facebook 'breaches Canadian law'. *BBC*. 2009. Available at: http://news.bbc.co.uk/1/hi/world/americas/8155367.stm. Accessed 13 Nov 2009.

Bennetto J. Police refuse to take DNA tests for database. The Independent. 2000.
Berthold O, Köhntopp M. Identity management based on P3P. In: Designing privacy enhancing technologies. 2001. p. 141–60. Available at: doi:10.1007/3-540-44702-4_9. Accessed 2 Aug 2010.
Bramhall P et al. User-centric identity management: new trends in standardization and regulation. IEEE Secur Privacy. 2007;5(4):84–7.
Burgoon J. Privacy and communication. In: Burgoon M, editor. Communication yearbook. Beverly Hills: Sage; 1982.
Camenisch J, et al. Privacy and identity management for everyone. In: Proceedings of the 2005 workshop on digital identity management. Fairfax, VA, USA: ACM; 2005. p. 20–7. Available at: http://portal.acm.org/citation.cfm?id=1102491. Accessed 2 Aug 2010.
Cameron K. The laws of identity. 2005. Available at: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.
Caplan J, Torpey JC. Documenting individual identity. Princeton University Press; 2001.
Carroll WC. Fat king, lean beggar: representations of poverty in the age of Shakespeare. Ithaca: Cornell University Press; 1996.
Cavoukian A. Privacy by design: take the challenge. Canada: Information and Privacy Commission of Ontario; 2009.
Cavoukian A. Privacy by design: the 7 foundational priniciples. 2010.
Criminal Justice and Police Act 2001, Available at: http://www.legislation.gov.uk/ukpga/2001/16/contents. Accessed 20 Aug 2010.
Davies SG. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In: Technology and privacy: the new landscape. MIT Press; 1997. p. 143–65. Available at: http://portal.acm.org/citation.cfm?id=275289. Accessed 16 Apr 2008.
Davies S. The complete ID primer. Index Censorsh. 2005;34(3):38.
Decew JW. In pursuit of privacy: law, ethics and the rise of technology. Cornell University Press; 1997.
DNA database call prompts concern. *BBC*. 2007. Available at: http://news.bbc.co.uk/1/hi/uk/6979490.stm. Accessed 20 Aug 2010.
DNA pioneer Alec Jeffreys: drop innocent from database | Politics | The Guardian. 2009. Available at: http://www.guardian.co.uk/politics/2009/apr/15/jeffreys-dna-database-human-rights-police. Accessed 28 June 2010.
Fishbein M. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading: Addison-Wesley Pub. Co.; 1975.
Fishbein M, Ajzen I. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading: Addison-Wesley Pub. Co.; 1975.
Flick U. An introduction to qualitative research. Sage; 2002.
Garfinkel SL, et al. How to make secure email easier to use. In: Proceedings of the SIGCHI conference on human factors in computing systems. Portland, Oregon, USA: ACM; 2005a. p. 701–10. Available at: http://portal.acm.org/citation.cfm?id=1055069. Accessed 28 June 2010.
Garfinkel SL, et al. How to make secure email easier to use. In: Proceedings of the SIGCHI conference on human factors in computing systems. Portland, Oregon, USA: ACM; 2005b. p. 701–10. Available at: http://portal.acm.org/citation.cfm?id=1055069. Accessed 30 June 2010.
Giddens A. The consequences of modernity. 1st ed. Stanford University Press; 1991.
Goldacre B. Bad science: Home Office research so feeble someone ought to be locked up | Ben Goldacre | Comment is free | The Guardian. 2009. Available at: http://www.guardian.co.uk/commentisfree/2009/jul/18/bad-science-dna-database. Accessed 20 Aug 2010.
Goldberg I. Privacy-enhancing technologies for the internet, II: five years later. In: Proceedings of the 2nd international conference on privacy enhancing technologies. San Francisco, CA, USA: Springer-Verlag; 2003. p. 1–12. Available at: http://portal.acm.org/citation.cfm?id=1765300. Accessed 2 Aug 2010.
Graham E. DNA reviews: the national DNA database of the United Kingdom. Forensic Sci Med Pathol. 2007;3(4):285–8.
Graham EAM. DNA reviews: low level DNA profiling. Forensic Sci Med Pathol. 2008;4(2):129–31.
Greenleaf G, Nolan J. The deceptive history of the 'Australia Card'. Aust Qtly. 1986;58(4):407–425.
Guardian. Phorm: UK faces court for failing to enforce EU privacy laws. 2009. Available at: http://www.guardian.co.uk/business/2009/apr/14/phorm-privacy-data-protection-eu. Accessed 16 Nov 2009.
Hayles NK. Waking up to the surveillance society. Surveillance & Society. 2009;6(3):313–6.
Hoadley CM, et al. Privacy as information access and illusory control: The case of the facebook news feed privacy outcry. Electronic commerce research and applications. 2009, in press, accepted manuscript. Available at: http://www.sciencedirect.com/science/article/B6X4K-4W85MD0-1/2/b4c518bb554d998aa61320944e40ca94. Accessed 15 May 2009.

Hope C. Omagh bomb verdict sparks DNA review. *Telegraph.co.uk*. 2007. Available at: http://www.telegraph.co.uk/news/uknews/1573269/Omagh-bomb-verdict-sparks-DNA-review.html. Accessed 17 Aug 2010.

Hope C. Millions of profiles from DNA database passed to private firms. *Telegraph.co.uk*. 2008. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/2459976/Millions-of-profiles-from-DNA-database-passed-to-private-firms.html. Accessed 29 June 2010.

Inglesant P, Sasse MA. Usability is the best policy: public policy and the lived experience of transport systems in London. In: Proceedings of the 21st British CHI Group Annual Conference on HCI 2007: People and Computers XXI: HCI:.but not as we know it—volume 1. University of Lancaster, United Kingdom: British Computer Society; 2007. p. 35–44. Available at: http://portal.acm.org/citation.cfm?id=1531294.1531300. Accessed 28 June 2010.

Jain AK, Bolle R, Pankanti S. Biometrics: personal identification in networked society. Springer; 1999.

Jøsang A, Zomai MA, Suriadi S. Usability and privacy in identity management architectures. In: Proceedings of the fifth Australasian symposium on ACSW frontiers—volume 68. Ballarat, Australia: Australian Computer Society, Inc.; 2007. p. 143–52. Available at: http://portal.acm.org/citation.cfm?id=1274548. Accessed 2 Aug 2010.

Leitold H, Posch K. Austria citizen card: a bottom up view. In: Jerman-Blažič B, et al., editors. 2004. p. 247.

Leitold H, Hollosi A, Posch R. Security architecture of the Austrian citizen card concept. In: Proceedings of 18th Annual Computer Security Applications Conference. 2002. p. 391–400. Available at: 10.1109/CSAC.2002.1176311. Accessed 19 Aug 2010.

Ley BL, Jankowski N, Brewer PR. Investigating CSI: portrayals of DNA testing on a forensic crime show and their potential effects. Public Underst. Sci. 2010. Available at: http://pus.sagepub.com/cgi/framedrapidpdf/0963662510367571v1?. Accessed 29 June 2010.

Lips M, Taylor J, Organ J. Personal identification and identity management in new modes of E-government. Oxford Internet Institute; 2005.

Lyon D. Surveillance society: monitoring everyday life. Buckingham: Open University Press; 2002.

Lyon D. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge; 2003.

Marks D, Yardley L. Research methods for clinical and health psychology. London: Thousand Oaks; 2004.

Martens T. Electronic identity management in Estonia between market and state governance. Identity in the Information Society. 2010;3. Available at: doi:10.1007/s12394-010-0044-0. Accessed 28 June 2010.

McCarthy J, Wright P. Technology as experience. Interactions. 2004;11(5):42–3.

Meints M, Hansen M. Study on ID documents. Future of Identity in the Information Society; 2006.

National Policing Improvement Agency. National DNA database annual report 2007–2009. 2010. Available at: http://www.npia.police.uk/en/14189.htm.

O'Donovan J, Smyth B. Trust in recommender systems. In: Proceedings of the 10th international conference on Intelligent user interfaces. San Diego, California, USA: ACM; 2005. p. 167–74. Available at: http://portal.acm.org/citation.cfm?id=1040830.1040870. Accessed 12 Aug 2010.

Omagh case review after verdict. *BBC*. 2007. Available at: http://news.bbc.co.uk/1/hi/northern_ireland/7149505.stm. Accessed 17 Aug 2010.

O'Neill S. DNA database under threat from European court, warns police chief. 2008. *The Times (UK)*. Available at: http://www.timesonline.co.uk/tol/news/uk/crime/article4083267.ece. Accessed 16 Aug 2010.

Orr J. Judge wants everyone in UK on DNA database | UK news | guardian.co.uk. 2007. Available at: http://www.guardian.co.uk/uk/2007/sep/05/humanrights.ukcrime. Accessed 28 June 2010.

Parliamentary Office of Science and Technology. The national DNA database. London: POST; 2006a.

Parliamentary Office of Science and Technology. The national DNA database. Parlimentary Office of Science and Technology. 2006b. Available at: http://www.parliament.uk/documents/upload/postpn258.pdf. Accessed 21 Nov 2008.

Pfitzmann A, Hansen M. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology. 2008. Available at: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf. Accessed 24 Apr 2008.

Rayner G, Gammell, C, Britten N. Madeleine McCann DNA 'an accurate match'. *Telegraph.co.uk*. 2008. Available at: http://www.telegraph.co.uk/news/worldnews/1562710/Madeleine-McCann-DNA-an-accurate-match.html. Accessed 28 June 2010.

Robbery conviction overturned. *BBC*. 1999. Available at: http://news.bbc.co.uk/1/hi/uk/258367.stm. Accessed 16 Aug 2010.

Science and Public Protection. Keeping the right people on the DNA Database. United Kingdom: Home Office; 2009.

Silcock R. What is E-government? Parliam Aff. 2001;54(1):88–101.

Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly. 1996;20(2):167–96.

Sokolov D. Österreichs größtem Signatur-Anbieter droht die Pleite. *Heise Online*. 2006a. Available at: http://translate.google.com/translate?hl=en&ie=UTF-8&u=http%3A%2F%2Fwww.heise.de%2Fnewsticker%2Fmeldung%2F68944&sl=de&tl=en&history_state0=.

Sokolov D. Österreichs Signaturanbieter A-Trust sucht den Weg aus der Krise. *Heise Online*. 2006b. Available at: http://www.heise.de/newsticker/Oesterreichs-Signaturanbieter-A-Trust-sucht-den-Weg-aus-der-Krise–/meldung/69316. Accessed 9 Jan 2009.

The Independent. The McCanns: unbelievable truth or unimaginable nightmare? The Independent. 2007. Available at: http://www.independent.co.uk/news/world/europe/the-mccanns-unbelievable-truth-or-unimaginable-nightmare-402486.html.

The Register. Japan rolls out national ID registry. The Register. 2002. Available at: http://www.theregister.co.uk/2002/08/07/japan_rolls_out_national_id/. Accessed 3 Apr 2008.

Thompson WC, Taroni F, Aitken CG. How the probability of a false positive affects the value of DNA evidence. J Forensic Sci. 2003;48(1):47–54.

Torpey J. The invention of the passport: surveliiance, citizenship and the state. Cambridge: Cambridge University Press; 2000.

Turow J, et al. Americans reject tailored advertising and three activities that enable it. In: SSRN eLibrary. AusCert. 2005. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214#. Accessed 16 Nov 2009.

Whitehead T. DNA fingerprint pioneer brands database ruling 'very disturbing'. *Telegraph.co.uk*. 2009. Available at: http://www.telegraph.co.uk/news/uknews/5293393/DNA-fingerprint-pioneer-brands-database-ruling-very-disturbing.html. Accessed 16 Aug 2010.

Workgroup on User-Centric Identity Management. Empowering individuals to control their personal informaiton. Wilmslow, United Kingdom: Information Commissioner's Office; 2008. Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/wgucidm_report.pdf.

Xin L. Trust in national identification systems: a trust model based on TRA/TPB. Washington State University; 2004. Available at: https://research.wsulibs.wsu.edu:8443/dspace/bitstream/2376/217/1/Xin_Li_071304.pdf. Accessed 31 Jan 2008.